Back Channels and BitCoins: ZeroAccess' Secret C&C Communications

VB2013

James Wyke

Senior Threat Researcher

SOPHOS

SOPHOS

Agenda

Agenda

- Brief Introduction to ZeroAccess
- Installation
- Tracker module
- Click fraud module
- BitCoin mining
- More click fraud
- Earnings
- Conclusion

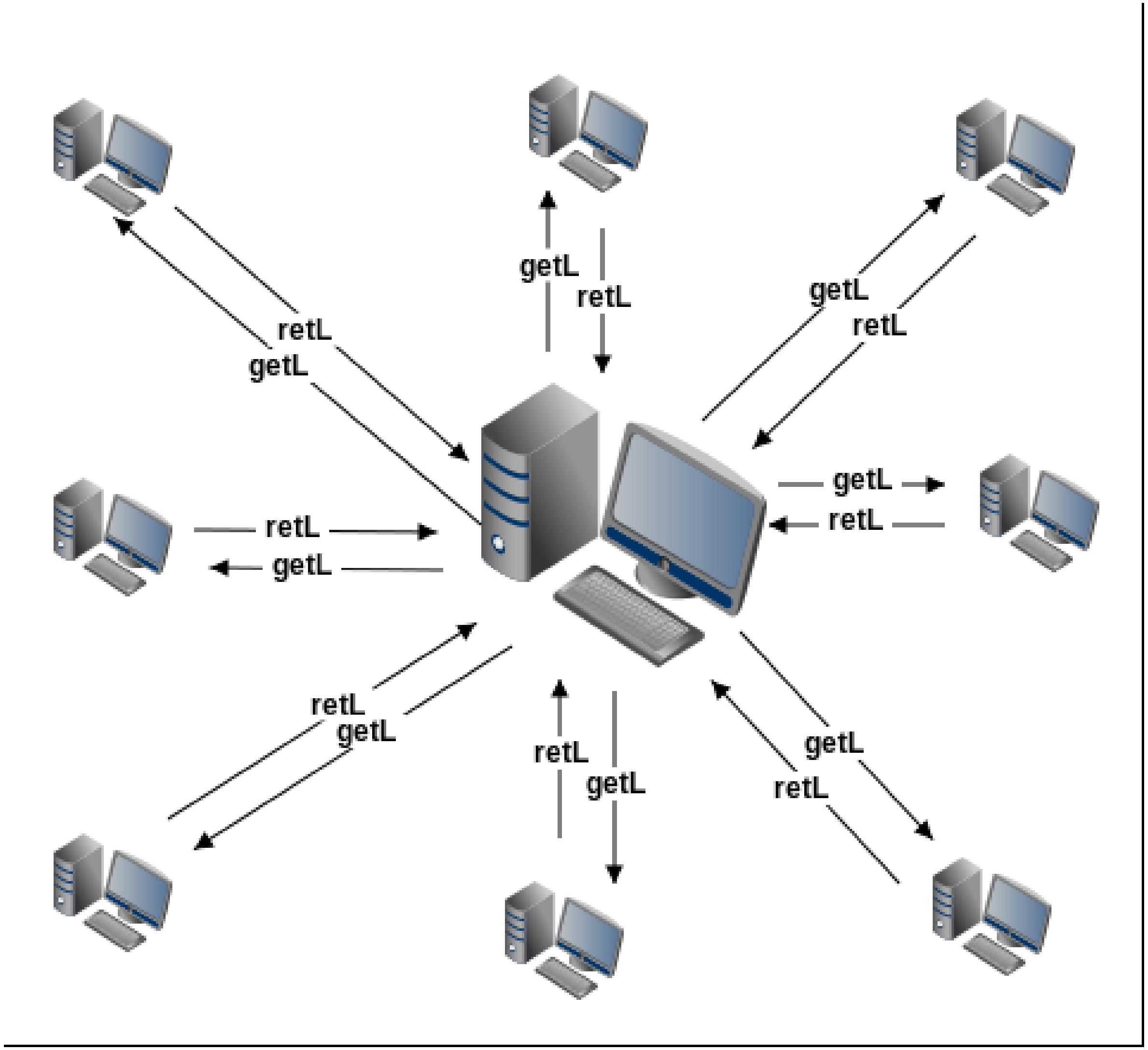
SOPHOS

Brief Introduction

Brief Introduction to ZeroAccess

- Custom P2P network spreads modules and peer addresses
- Modules carry out payload functionality
- User-mode and kernel-mode
- Very noisy from network perspective

P2P Network


getL
retL
getL
retL
retL
getL
getL
retL
retL
getL
retL
getL
retL
getL
getL
retL

P2P Network cont.

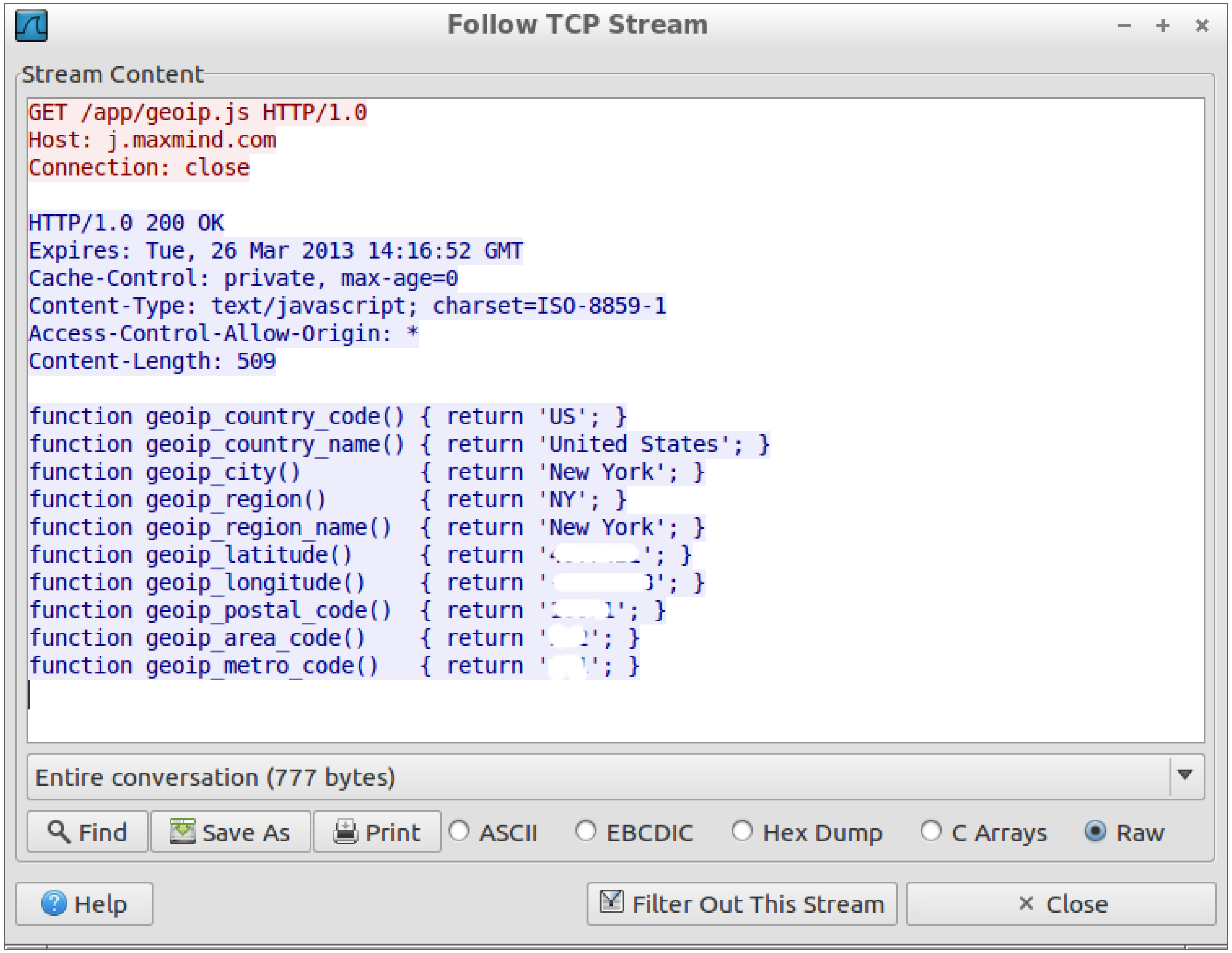
- *getL* to retrieve peer and file list
- *retL* contains response to *getL*
- One *getL* per second, 80,000+ per day
- Fixed port numbers
- Noise masks other communications

Installation

Installation

- Dropper phones home
- GEOIP lookup
- HTTP Get request
- Encrypted packet on UDP port 53
- Feed affiliate program
- Record information on infected machines

GEOIP Lookup



```
GET /app/geoip.js HTTP/1.0
Host: j.maxmind.com
Connection: close

HTTP/1.0 200 OK
Expires: Tue, 26 Mar 2013 14:16:52 GMT
Cache-Control: private, max-age=0
Content-Type: text/javascript; charset=ISO-8859-1
Access-Control-Allow-Origin: *
Content-Length: 509

function geoip_country_code() { return 'US'; }
function geoip_country_name() { return 'United States'; }
function geoip_city()         { return 'New York'; }
function geoip_region()       { return 'NY'; }
function geoip_region_name()  { return 'New York'; }
function geoip_latitude()     { return '[redacted]'; }
function geoip_longitude()    { return '[redacted]'; }
function geoip_postal_code()  { return '[redacted]'; }
function geoip_area_code()    { return '[redacted]'; }
function geoip_metro_code()   { return '[redacted]'; }
```

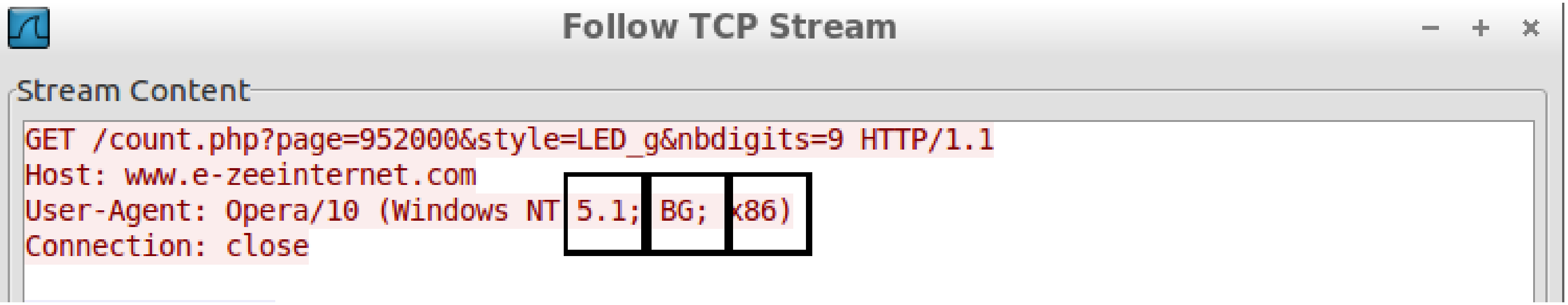
Entire conversation (777 bytes)

○ ASCII ○ EBCDIC ○ Hex Dump ○ C Arrays ● Raw

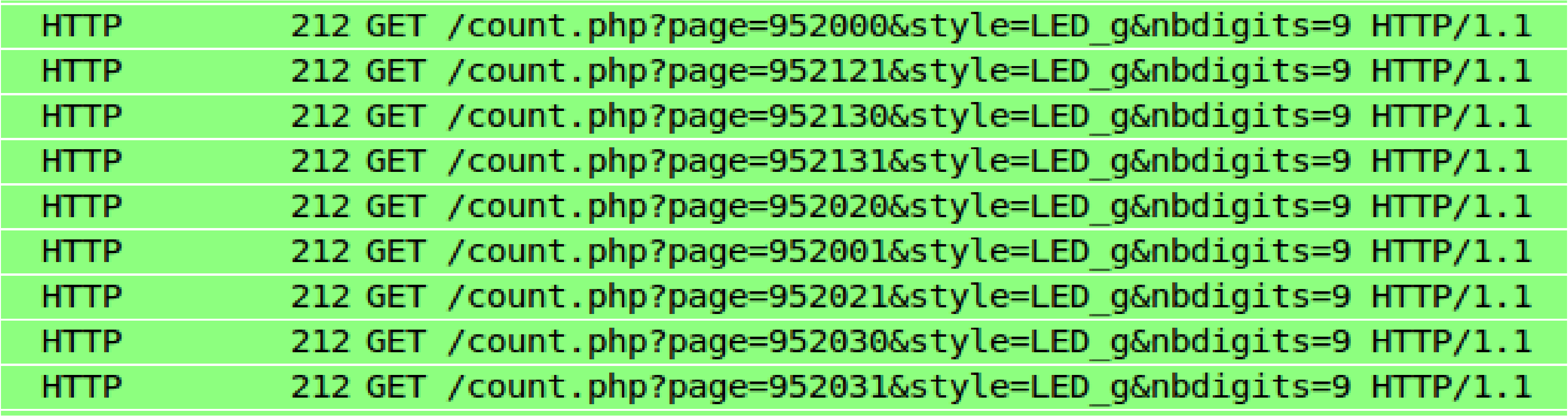
HTTP Get Request

- Web counter URL
- Infected machine information encoded in headers
- Multiple requests made – URL modified as execution proceeds
- Counter increments with each hit

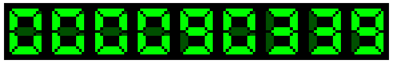
HTTP Get Request cont.



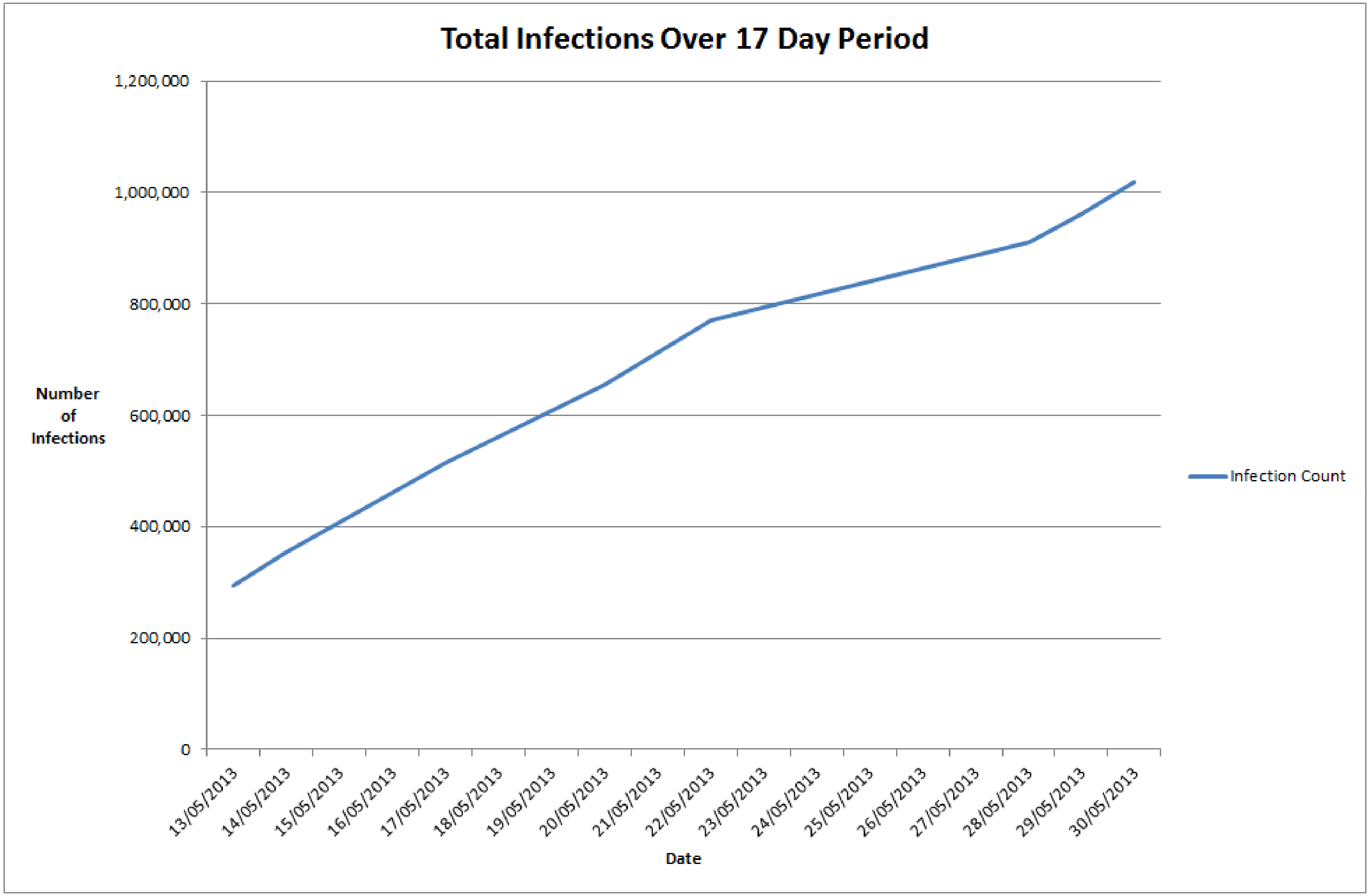
```
GET /count.php?page=952000&style=LED_g&nbdigits=9 HTTP/1.1
Host: www.e-zeeinternet.com
User-Agent: Opera/10 (Windows NT 5.1; BG; x86)
Connection: close
```



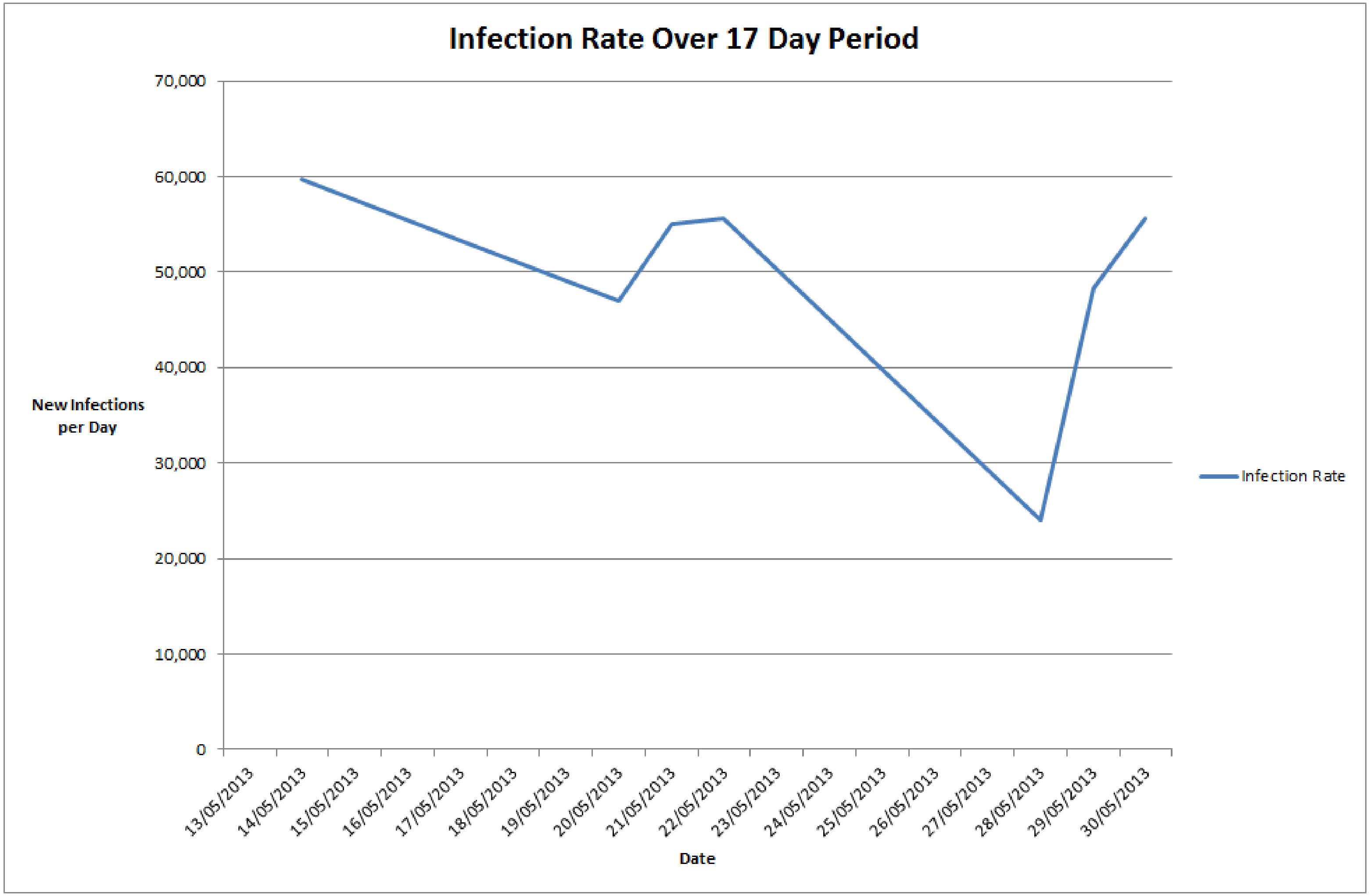
```
HTTP        212 GET /count.php?page=952000&style=LED_g&nbdigits=9 HTTP/1.1
HTTP        212 GET /count.php?page=952121&style=LED_g&nbdigits=9 HTTP/1.1
HTTP        212 GET /count.php?page=952130&style=LED_g&nbdigits=9 HTTP/1.1
HTTP        212 GET /count.php?page=952131&style=LED_g&nbdigits=9 HTTP/1.1
HTTP        212 GET /count.php?page=952020&style=LED_g&nbdigits=9 HTTP/1.1
HTTP        212 GET /count.php?page=952001&style=LED_g&nbdigits=9 HTTP/1.1
HTTP        212 GET /count.php?page=952021&style=LED_g&nbdigits=9 HTTP/1.1
HTTP        212 GET /count.php?page=952030&style=LED_g&nbdigits=9 HTTP/1.1
HTTP        212 GET /count.php?page=952031&style=LED_g&nbdigits=9 HTTP/1.1
```



HTTP Get Request cont.



HTTP Get Request cont.

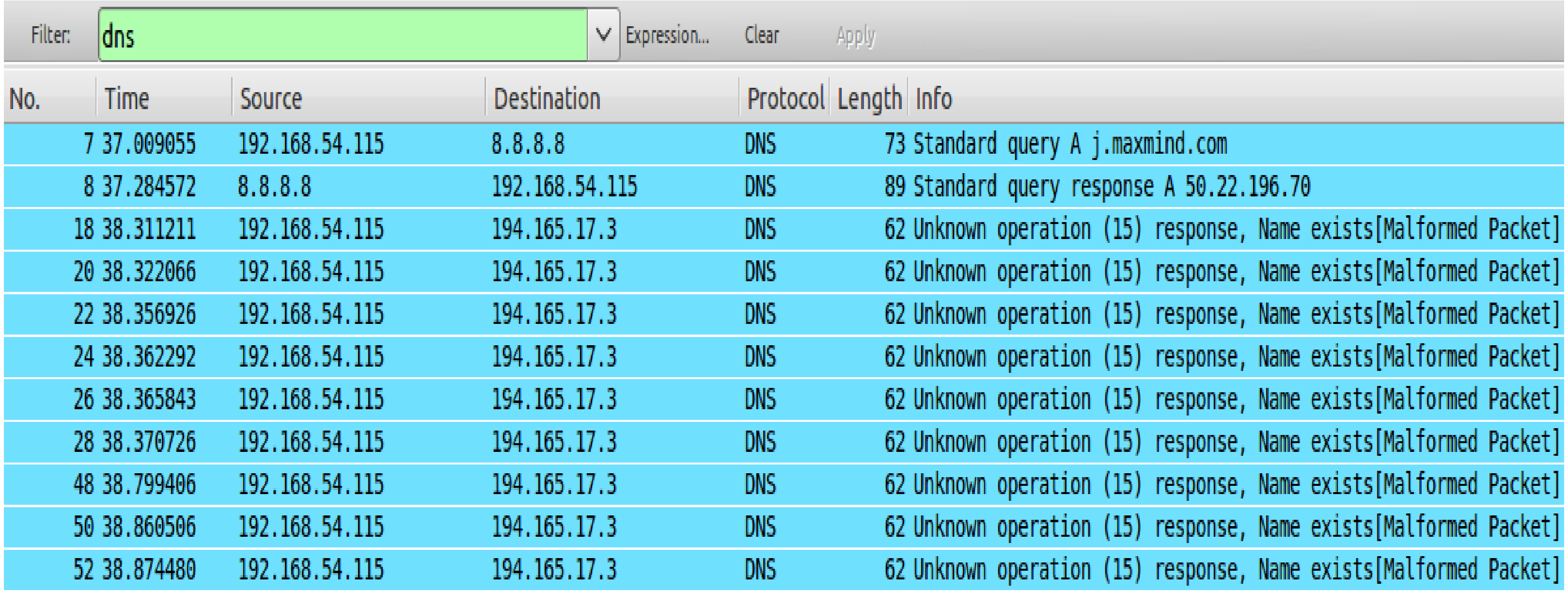


HTTP Get Request cont.

- One portion of the botnet
- Average of 49,000 new infections per day
- In 2012, full botnet averages 140,000 per day

UDP Port 53

- Same information as HTTP Request
- Disguised as malformed DNS data



Filter: dns

No.	Time	Source	Destination	Protocol	Length	Info
7	37.009055	192.168.54.115	8.8.8.8	DNS	73	Standard query A j.maxmind.com
8	37.284572	8.8.8.8	192.168.54.115	DNS	89	Standard query response A 50.22.196.70
18	38.311211	192.168.54.115	194.165.17.3	DNS	62	Unknown operation (15) response, Name exists[Malformed Packet]
20	38.322066	192.168.54.115	194.165.17.3	DNS	62	Unknown operation (15) response, Name exists[Malformed Packet]
22	38.356926	192.168.54.115	194.165.17.3	DNS	62	Unknown operation (15) response, Name exists[Malformed Packet]
24	38.362292	192.168.54.115	194.165.17.3	DNS	62	Unknown operation (15) response, Name exists[Malformed Packet]
26	38.365843	192.168.54.115	194.165.17.3	DNS	62	Unknown operation (15) response, Name exists[Malformed Packet]
28	38.370726	192.168.54.115	194.165.17.3	DNS	62	Unknown operation (15) response, Name exists[Malformed Packet]
48	38.799406	192.168.54.115	194.165.17.3	DNS	62	Unknown operation (15) response, Name exists[Malformed Packet]
50	38.860506	192.168.54.115	194.165.17.3	DNS	62	Unknown operation (15) response, Name exists[Malformed Packet]
52	38.874480	192.168.54.115	194.165.17.3	DNS	62	Unknown operation (15) response, Name exists[Malformed Packet]

Tracker Module

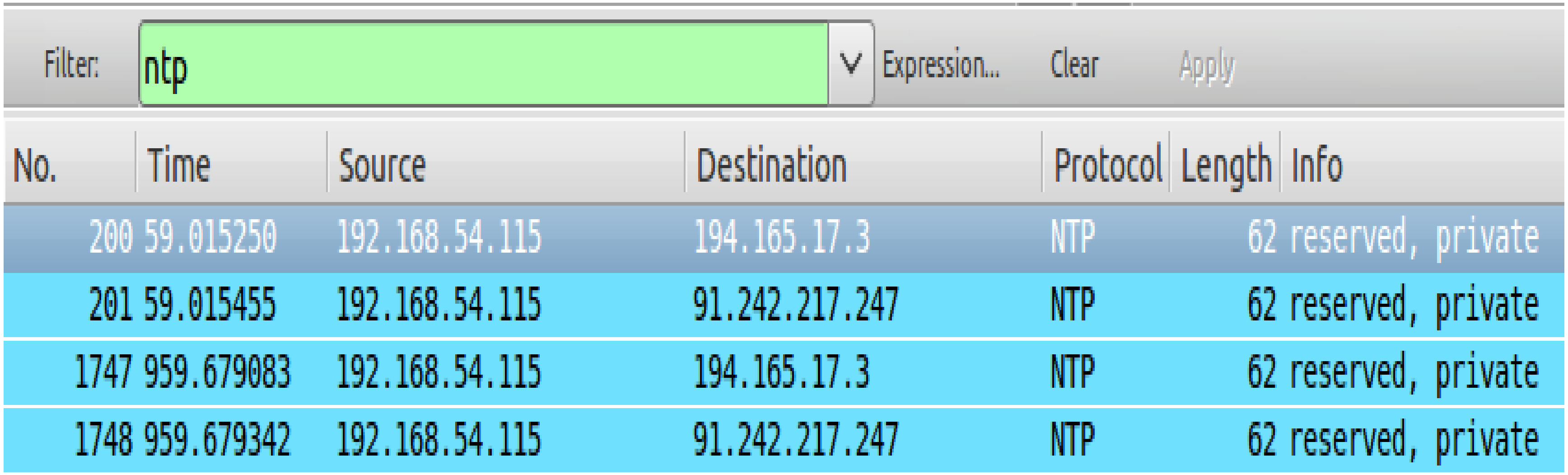
Tracker Module

- *80000000* - Downloaded by every botnet
- Sends back infected machine information every 15 minutes
- Fill new peer lists with live peers
- Dynamically retrieved address
- Disguised as NTP traffic

Tracker Module

Offset	Value
0x0	Intentionally Zero
0x2	Country code of externally facing IP
0x4	Encoded version of the current day
0x6	User privilege level + version modifier
0x7	OS version Info
0x8	Affiliate ID
0xc	BotID
0x10	CRC32 of data (Zero before CRC)

Tracker Module



No.	Time	Source	Destination	Protocol	Length	Info
200	59.015250	192.168.54.115	194.165.17.3	NTP	62	reserved, private
201	59.015455	192.168.54.115	91.242.217.247	NTP	62	reserved, private
1747	959.679083	192.168.54.115	194.165.17.3	NTP	62	reserved, private
1748	959.679342	192.168.54.115	91.242.217.247	NTP	62	reserved, private

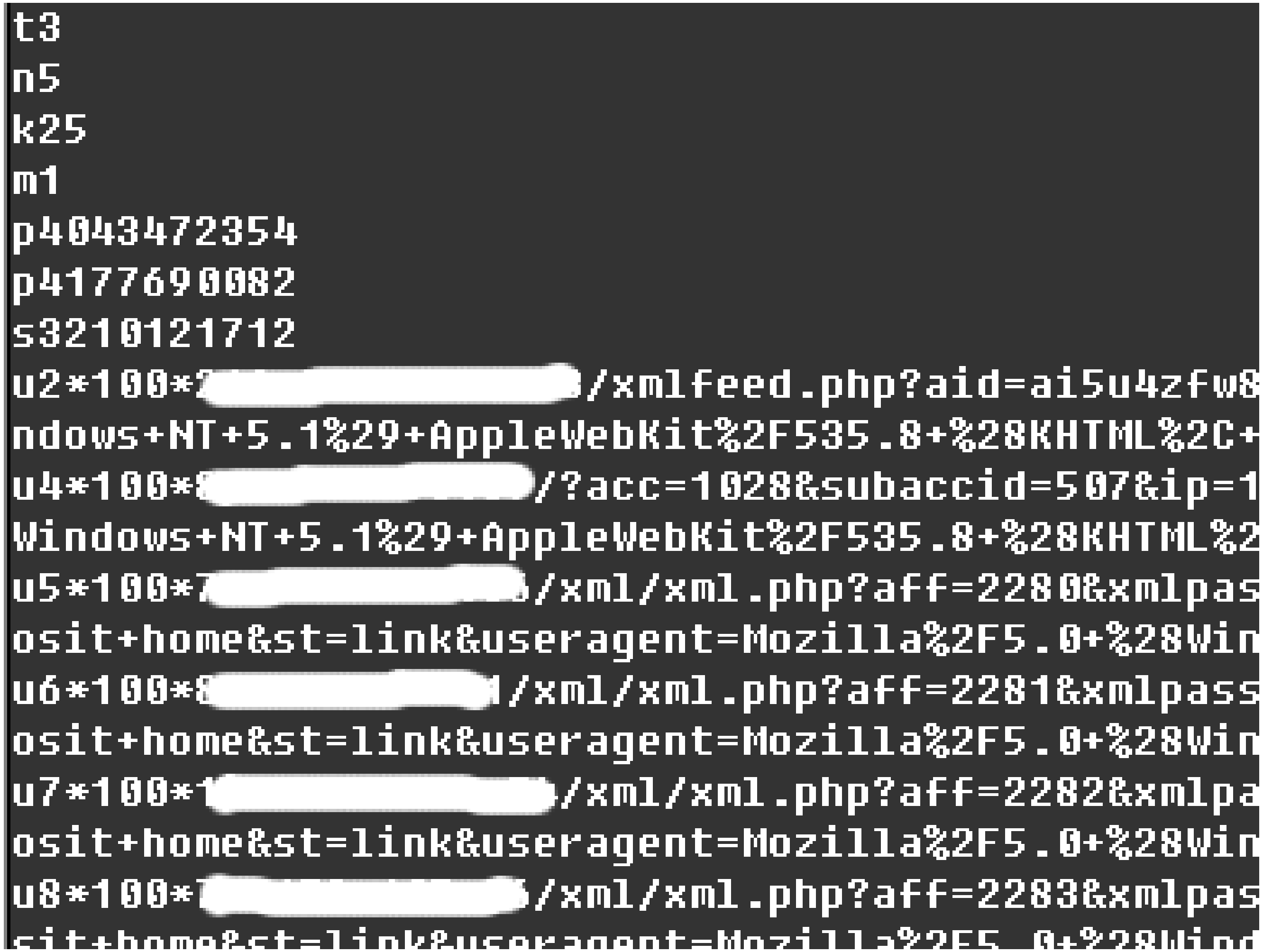
SOPHOS

Click Fraud Module

Click Fraud Module

- *800000cb* – downloaded by botnets running on ports 16464 and 16465
- Several revisions
- Spoofed host field – DGA
- Historic use of decoy URLs

Decoy URLs



```
t3
n5
k25
m1
p4043472354
p4177690082
s3210121712
u2*100*[redacted]/xmlfeed.php?aid=ai5u4zfw&
ndows+NT+5.1%29+AppleWebKit%2F535.8+%28KHTML%2C+
u4*100*[redacted]/?acc=1028&subaccid=507&ip=1
Windows+NT+5.1%29+AppleWebKit%2F535.8+%28KHTML%2
u5*100*[redacted]/xml/xml.php?aff=2280&xmlpas
osit+home&st=link&useragent=Mozilla%2F5.0+%28Win
u6*100*[redacted]/xml/xml.php?aff=2281&xmlpass
osit+home&st=link&useragent=Mozilla%2F5.0+%28Win
u7*100*[redacted]/xml/xml.php?aff=2282&xmlpa
osit+home&st=link&useragent=Mozilla%2F5.0+%28Win
u8*100*[redacted]/xml/xml.php?aff=2283&xmlpas
sit+home&st=link&useragent=Mozilla%2F5.0+%28Wind
```

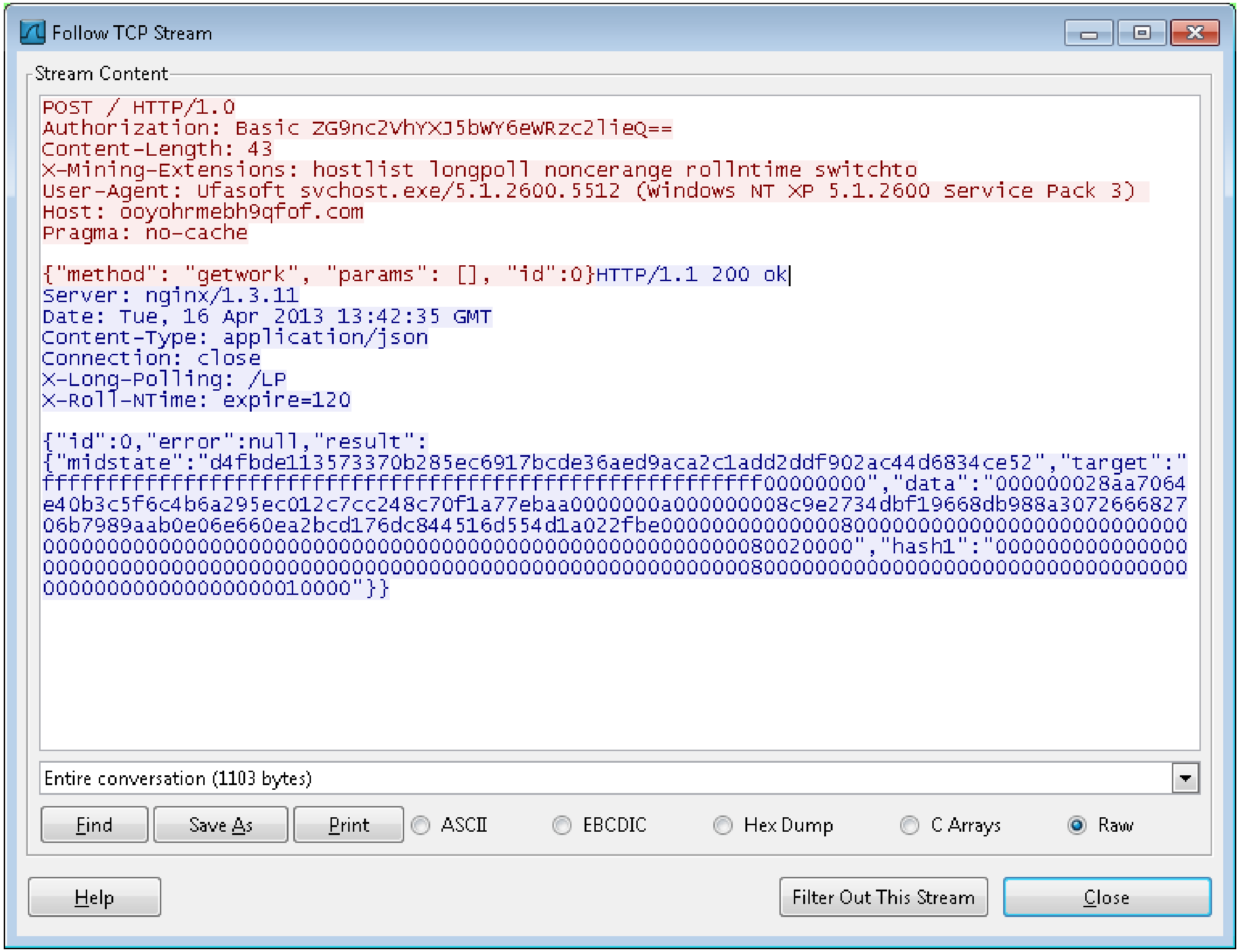
SOPHOS

BitCoin Mining

BitCoin Mining

- Botnets on port 16470 and 16471 – *00000008* module
- *UfaSoft* miner
- Pushpool mining pool
- JSON data

BitCoin Mining cont.



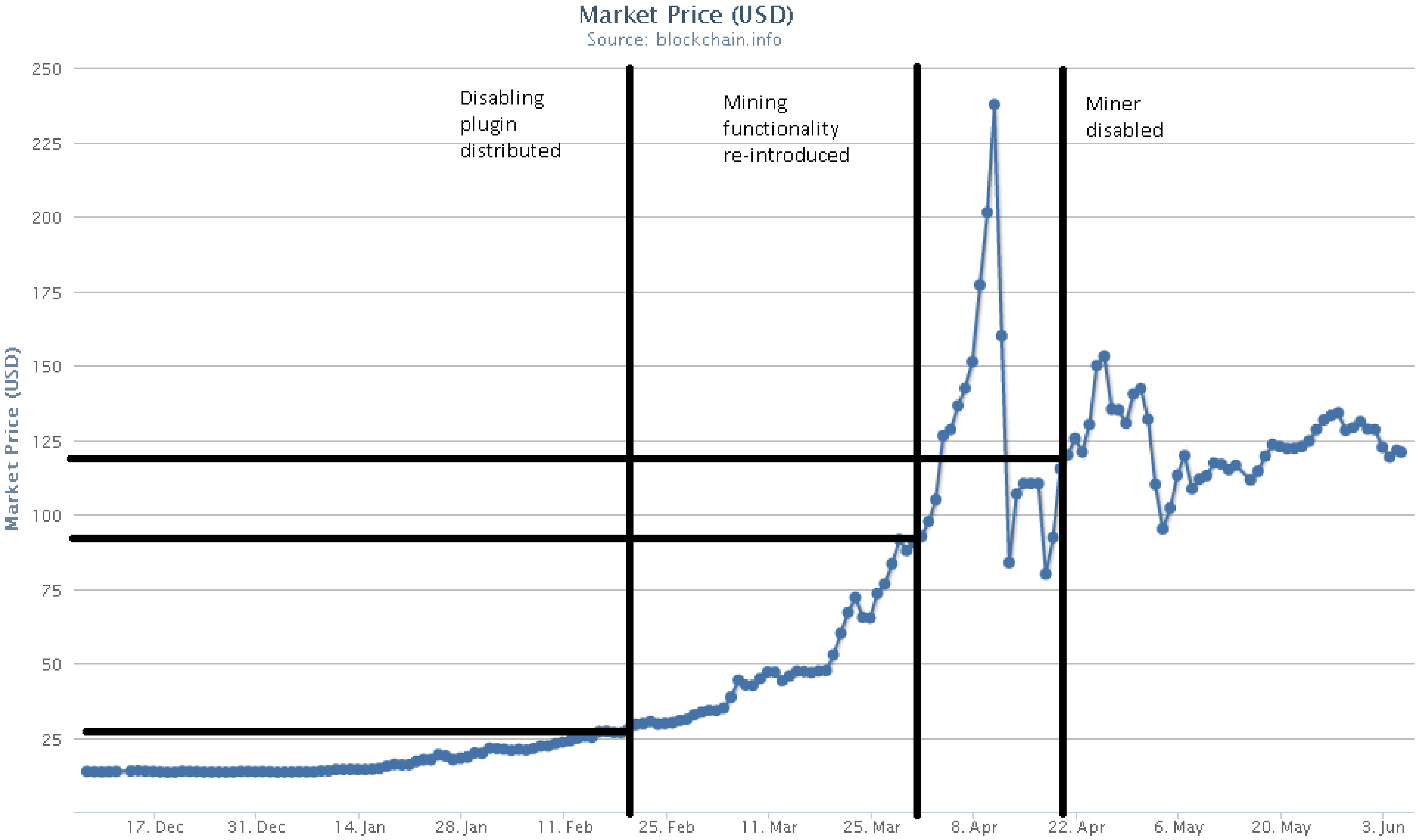
```
POST / HTTP/1.0
Authorization: Basic ZG9nc2VhYXJ5bWY6eWRzc2lieQ==
Content-Length: 43
X-Mining-Extensions: hostlist longpoll noncerange rollntime switchto
User-Agent: Ufasoft svchost.exe/5.1.2600.5512 (Windows NT XP 5.1.2600 Service Pack 3)
Host: ooyohrmebh9qfof.com
Pragma: no-cache

{"method": "getwork", "params": [], "id":0}HTTP/1.1 200 ok
Server: nginx/1.3.11
Date: Tue, 16 Apr 2013 13:42:35 GMT
Content-Type: application/json
Connection: close
X-Long-Polling: /LP
X-Roll-NTime: expire=120

{"id":0,"error":null,"result":
{"midstate":"d4fbde113573370b285ec6917bcde36aed9aca2c1add2ddf902ac44d6834ce52","target":"
ffffffffffffffffffffffffffffffffffffffffffffffffffffffff00000000","data":"00000028aa7064
e40b3c5f6c4b6a295ec012c7cc248c70f1a77ebaa0000000a000000008c9e2734dbf19668db988a3072666827
06b7989aab0e06e660ea2bcd176dc844516d554d1a022fbe0000000000000008000000000000000000000000
0000000000000000000000000000000000000000000000000000000080020000","hash1":"000000000000000
000000000000000000000000000000000000000000000000000000008000000000000000000000000000000000
0000000000000000000010000"}}
```

Entire conversation (1103 bytes)

BitCoin Mining cont.

- Exchange rate fluctuations affect ZeroAccess
- Initial timestamp: 12 May 2012 06:52:40 GMT
- No update for over 9 months
- Module disabled prior to early 2013 price boom
- Re-enabled and updated when price nears $100
- Disabled again 1 month later

BitCoin Mining cont.



Disabling plugin distributed

Mining functionality re-introduced

Miner disabled

Why Disable the BitCoin Miner?

- Currency too unstable?
- Too difficult to cash out?
- Too much attention?

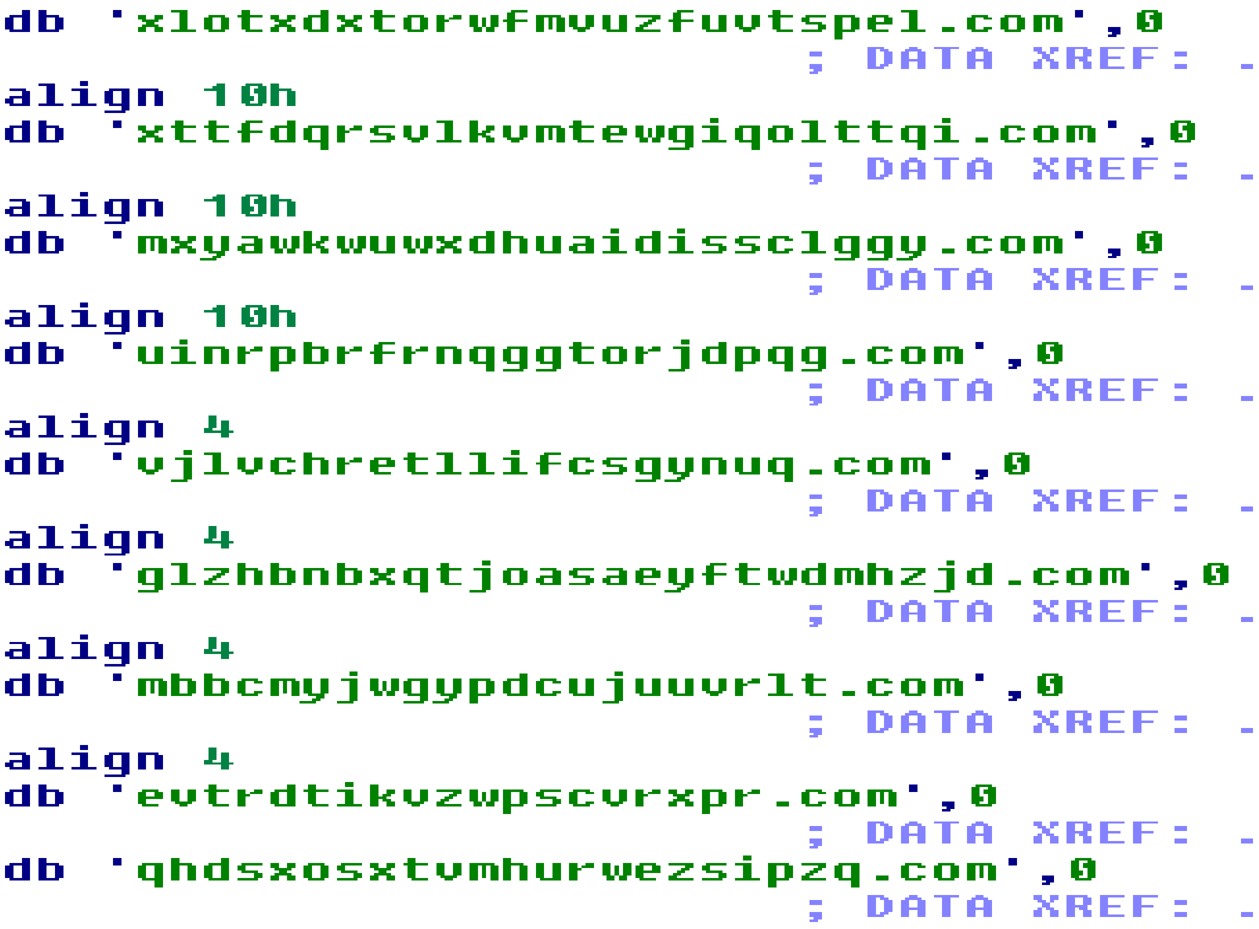
SOPHOS

More Click Fraud

More Click Fraud

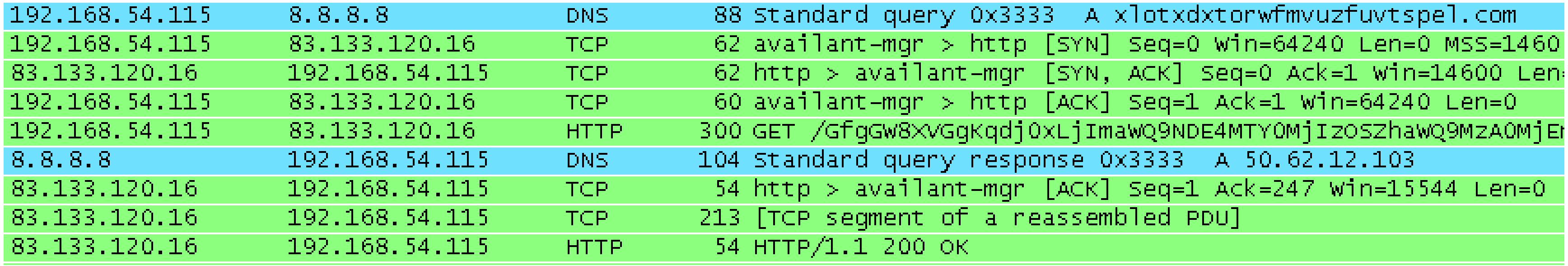
- *80000032* and *80000064*
- Click fraud and file download
- Outbound HTTP request spoofs Host: field
- Complicate PCAP analysis
- Any intercepting proxy will generate a request to an incorrect address

Spoofed Domains



```
db 'xlotxdxtorwfmvuzfuvtspel.com',0
                         ; DATA XREF: .
align 10h
db 'xttfdqrsvlkvmtewgiqolttqi.com',0
                         ; DATA XREF: .
align 10h
db 'mxyawkwuwxdhuaidissclggy.com',0
                         ; DATA XREF: .
align 10h
db 'uinrpbrfrnqggtorjdpqg.com',0
                         ; DATA XREF: .
align 4
db 'vjlvchretllifcsgynuq.com',0
                         ; DATA XREF: .
align 4
db 'glzhbnbxqtjoasaeyftwdmhzjd.com',0
                         ; DATA XREF: .
align 4
db 'mbbcmyjwgypdcujuuvrlt.com',0
                         ; DATA XREF: .
align 4
db 'evtrdtikvzwpscvrxpr.com',0
                         ; DATA XREF: .
db 'qhdsxosxtvmhurwezsipzq.com',0
                         ; DATA XREF: .
```

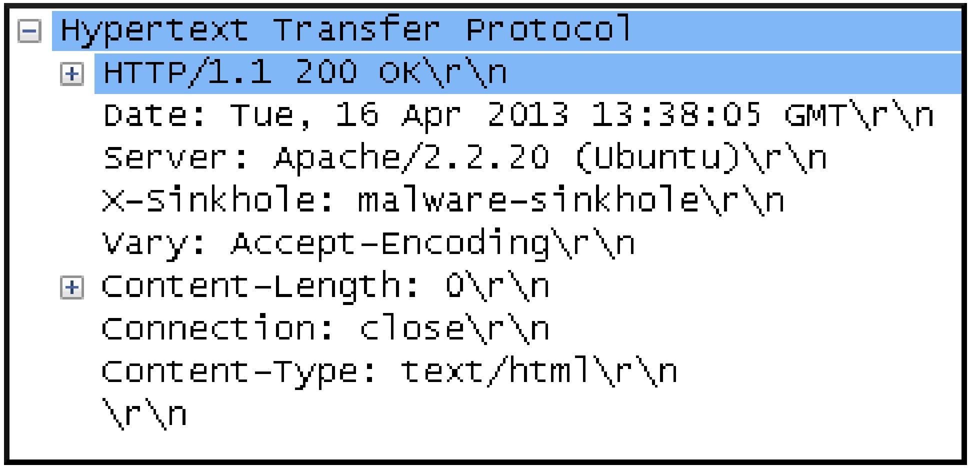
Ignored DNS Request



```
192.168.54.115     8.8.8.8            DNS        88 Standard query 0x3333  A xlotxdxtorwfmvuzfuvtspel.com
192.168.54.115     83.133.120.16      TCP        62 availant-mgr > http [SYN] Seq=0 Win=64240 Len=0 MSS=1460
83.133.120.16      192.168.54.115     TCP        62 http > availant-mgr [SYN, ACK] Seq=0 Ack=1 Win=14600 Len
192.168.54.115     83.133.120.16      TCP        60 availant-mgr > http [ACK] Seq=1 Ack=1 Win=64240 Len=0
192.168.54.115     83.133.120.16      HTTP      300 GET /GfgGW8XVGgKqdj0xLjImaWQ9NDE4MTY0MjIzOSZhaWQ9MzA0MjE
8.8.8.8            192.168.54.115     DNS       104 Standard query response 0x3333  A 50.62.12.103
83.133.120.16      192.168.54.115     TCP        54 http > availant-mgr [ACK] Seq=1 Ack=247 Win=15544 Len=0
83.133.120.16      192.168.54.115     TCP       213 [TCP segment of a reassembled PDU]
83.133.120.16      192.168.54.115     HTTP       54 HTTP/1.1 200 OK
```

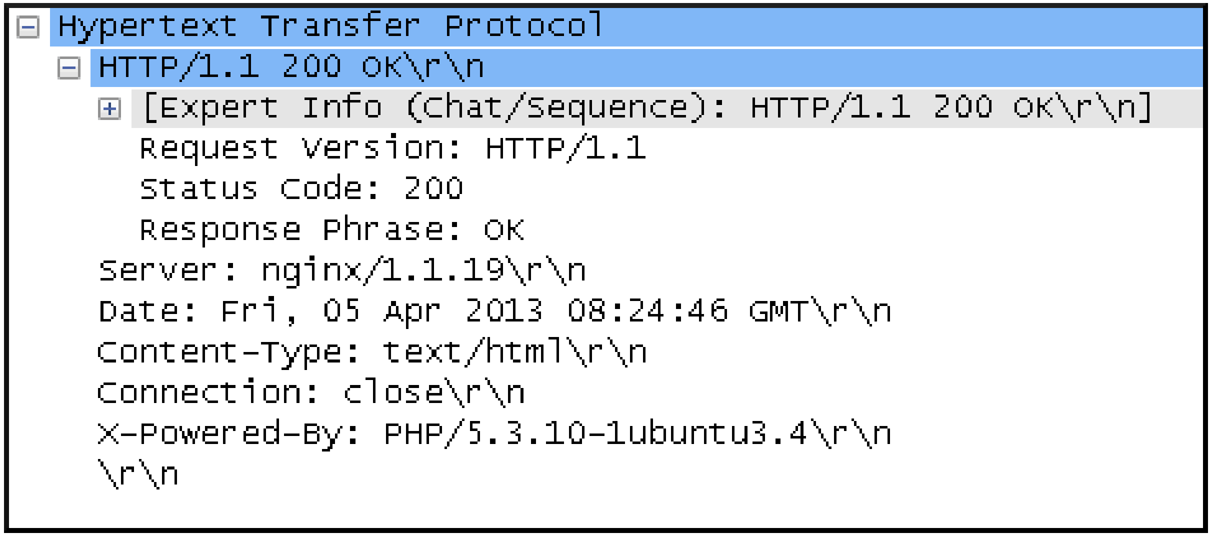
Fake Domain Sinkholed

- Sinkhole:



```
⊟ Hypertext Transfer Protocol
  ⊞ HTTP/1.1 200 OK\r\n
    Date: Tue, 16 Apr 2013 13:38:05 GMT\r\n
    Server: Apache/2.2.20 (Ubuntu)\r\n
    X-Sinkhole: malware-sinkhole\r\n
    Vary: Accept-Encoding\r\n
  ⊞ Content-Length: 0\r\n
    Connection: close\r\n
    Content-Type: text/html\r\n
    \r\n
```

- Genuine:



```
⊟ Hypertext Transfer Protocol
  ⊟ HTTP/1.1 200 OK\r\n
    ⊞ [Expert Info (Chat/Sequence): HTTP/1.1 200 OK\r\n]
      Request Version: HTTP/1.1
      Status Code: 200
      Response Phrase: OK
    Server: nginx/1.1.19\r\n
    Date: Fri, 05 Apr 2013 08:24:46 GMT\r\n
    Content-Type: text/html\r\n
    Connection: close\r\n
    X-Powered-By: PHP/5.3.10-1ubuntu3.4\r\n
    \r\n
```

SOPHOS

Earnings

Earnings - BitCoin

- 500,000 nodes at 4Mhash/s = 2,000 Ghash/s

Dollars per BitCoin	Revenue per Day ($)
10	644.53
25	1,611.32
100	6,445.29
200	12,890.58

- **Disabled**

Earnings – Click Fraud

- Favoured monetization method
- $90,000 - $200,000 per day
- *The ZeroAccess Botnet: Mining and Fraud for Massive Financial Gain*
- *Chameleon Botnet - http://www.spider.io/blog/2013/03/chameleon-botnet/*

SOPHOS

Conclusion

Conclusion

- Resilient and long-lasting Botnet
- Widespread – huge number of new installs each day
- Adaptable – updates to resist sinkholing
- Use of misdirection
- Masquerade as legitimate traffic
- Attempts to stay under the radar

SOPHOS