Kelihos Botnet

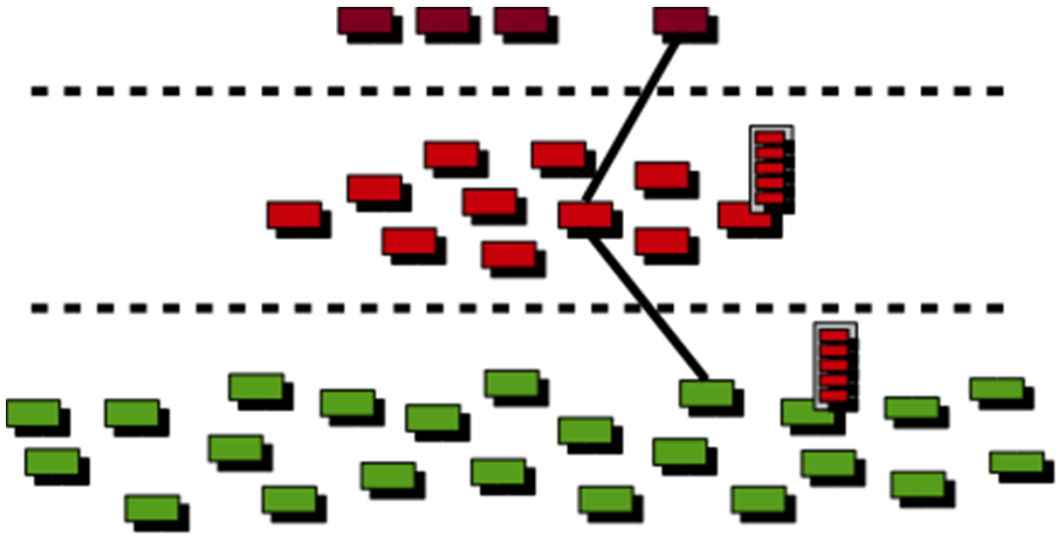
Stirling Algermissen

“Kelihos botnet, once crippled, now gaining strength”

- Allegedly developed by Andrey N. Sabelnikov of St. Petersburg
- ~50,000 machines compromised
- Targeted by Microsoft and Kaspersky Lab for disruption
- Botnet still exists

How Kelihos Functions

- Peer to peer
- 3 layers – controllers, routers, and workers
- Controllers – distribute commands and supervise network
- Router – public IP's that are proxies
- Workers – send spam, collect email addresses



Worker Nodes

- Often times behind a gateway, proxy or other device that performs network translation
- Checks if publically connectable
- Maintains list of peers and requests jobs from them
- Jobs include sending spam, collecting email addresses to send spam, and participating in denial of service

Router Nodes

- “some kind of backbone layer in the Kelihos botnet” - securelist
- Each router maintains a list of peers like a worker node and also maintains a list of controllers
- Also acts as an HTTP proxy for workers
- Routers can execute jobs but their primary purpose is to provide a proxy layer in front of the controllers
- Participate in fast flux

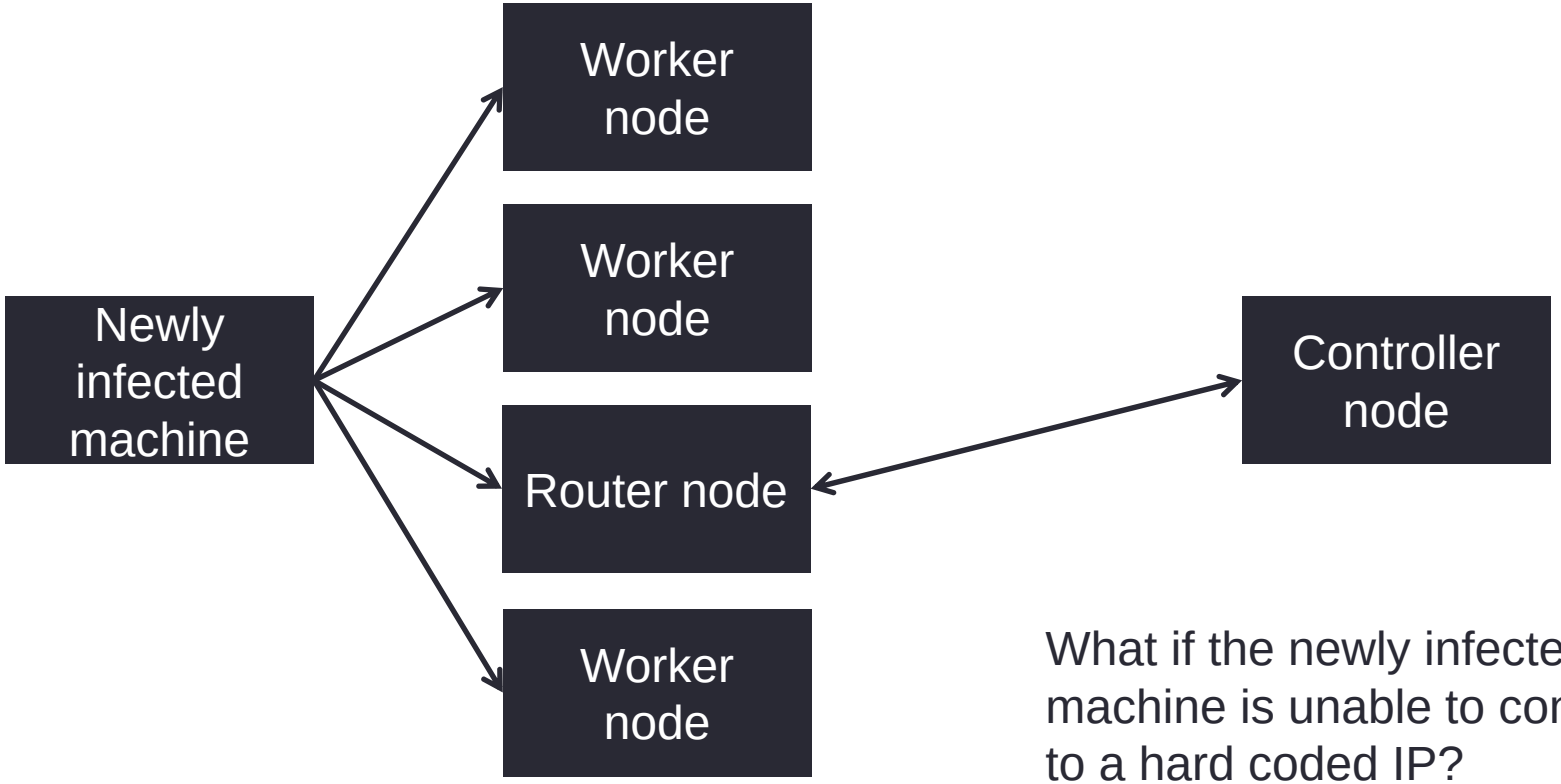
Controller Nodes

- Host a nginx HTTP server and serve job messages
- Do not take part in the P2P botnet – never show up in peer lists
- 6 of them, spread pairwise over different IP ranges in different countries

```
Controller IP addresses:
193.105.134.189
193.105.134.190
195.88.191.55
195.88.191.57
89.46.251.158
89.46.251.160
```

The P2P Network

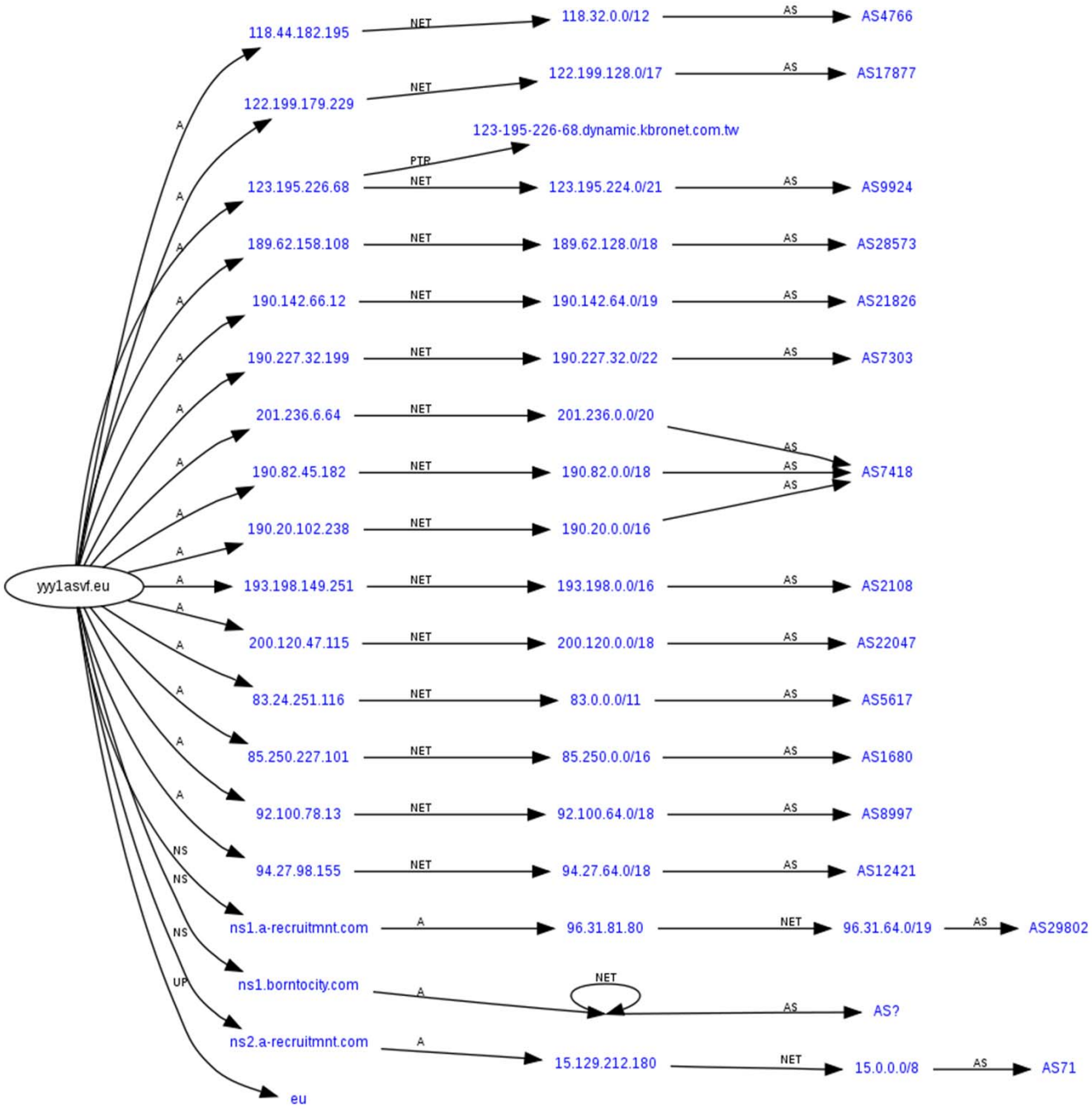
```
m_ip: 41.212.81.2
m_live_time: 22639 seconds
m_last_active_time: 2011-09-08 11:24:26 GMT
m_listening_port: 80
m_client_id: cbd47c00-f240-4c2b-9131-ceea5f4b7f67
```



What if the newly infected machine is unable to connect to a hard coded IP?

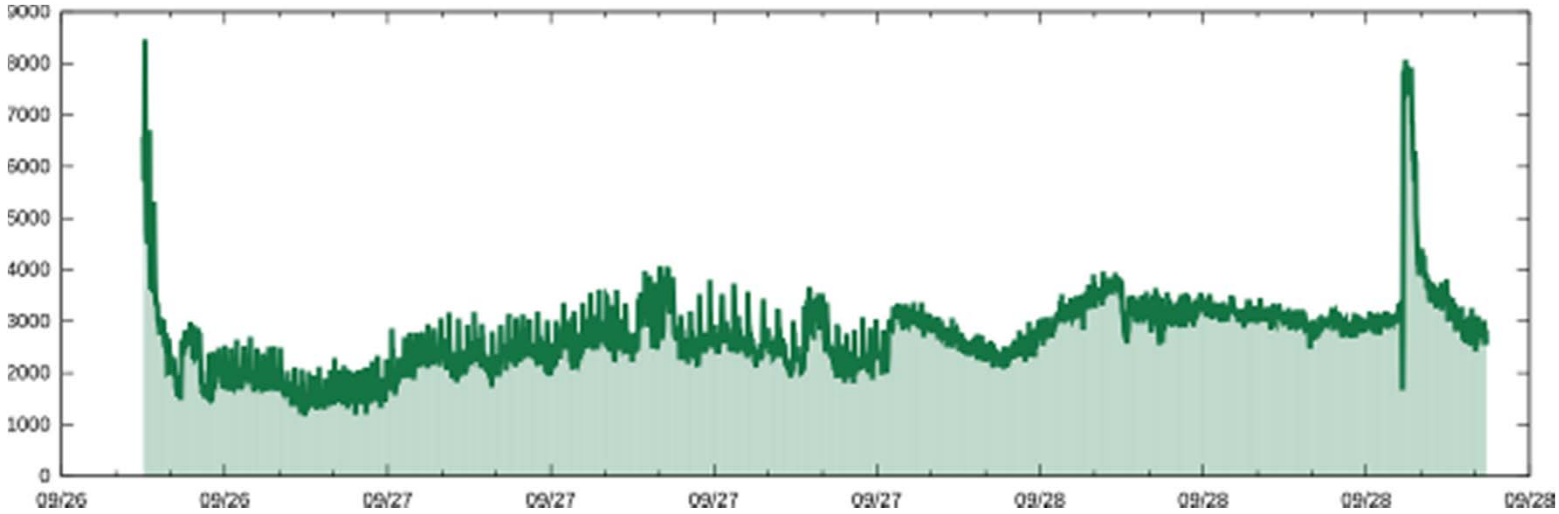
The Fast-Flux Service Network

- DNS technique – have numerous IP addresses associated with a single fully qualified domain name
- Router IP addresses are swapped in and out with extremely high frequency through changing DNS records
- Worker node uses this system to connect to the botnet if every hardcoded IP is down
- Hundreds of domains names used
- Microsoft unregistered these domains

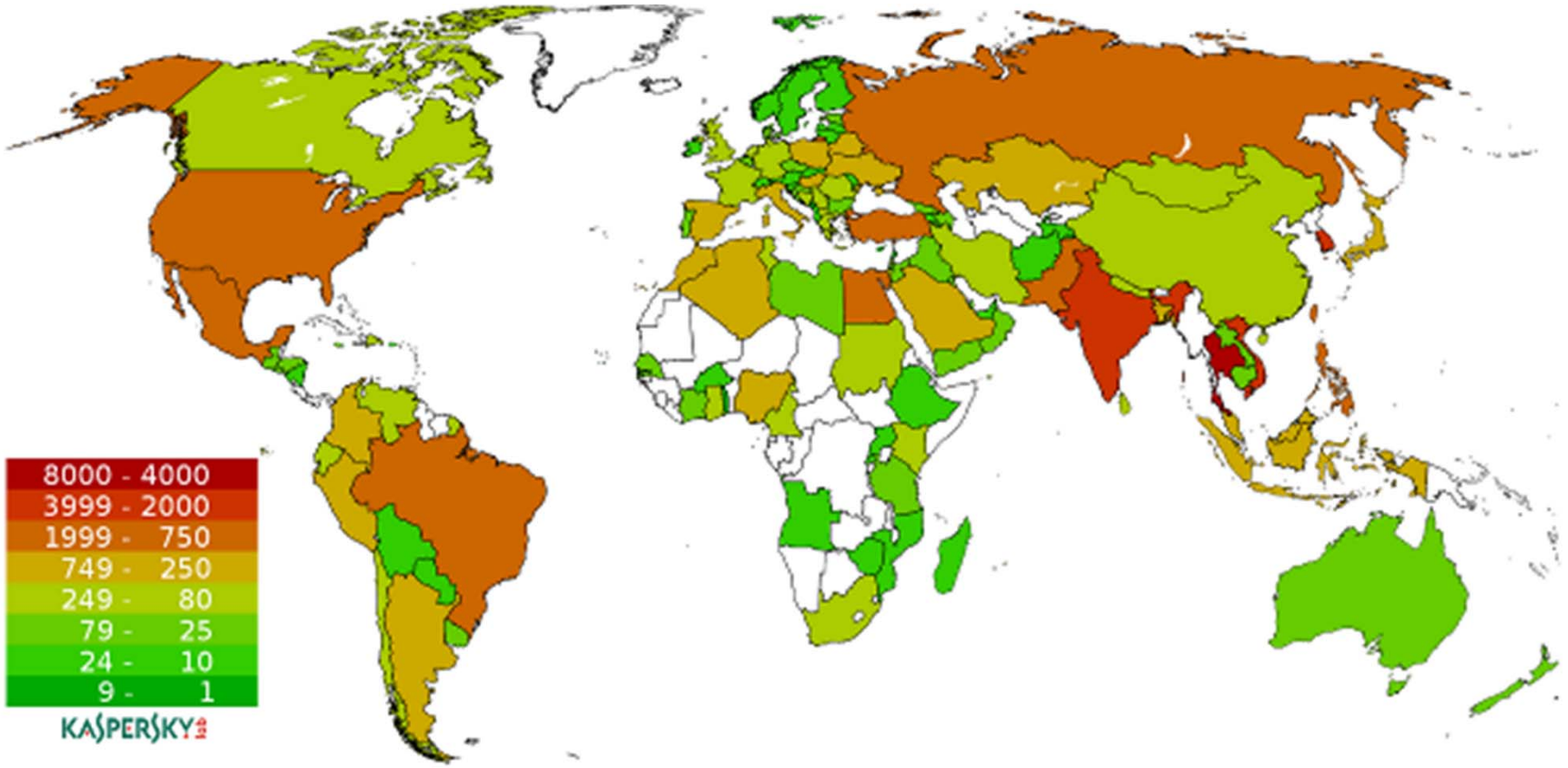

yyy1asvf.eu
118.44.182.195
122.199.179.229
123.195.226.68
189.62.158.108
190.142.66.12
190.227.32.199
201.236.6.64
190.82.45.182
190.20.102.238
193.198.149.251
200.120.47.115
83.24.251.116
85.250.227.101
92.100.78.13
94.27.98.155
ns1.a-recruitmnt.com
ns1.borntocity.com
ns2.a-recruitmnt.com
eu
A
NS
UP
NET
PTR
AS
118.32.0.0/12
AS4766
122.199.128.0/17
AS17877
123-195-226-68.dynamic.kbronet.com.tw
123.195.224.0/21
AS9924
189.62.128.0/18
AS28573
190.142.64.0/19
AS21826
190.227.32.0/22
AS7303
201.236.0.0/20
190.82.0.0/18
190.20.0.0/16
AS7418
193.198.0.0/16
AS2108
200.120.0.0/18
AS22047
83.0.0.0/11
AS5617
85.250.0.0/16
AS1680
92.100.64.0/18
AS8997
94.27.64.0/18
AS12421
96.31.81.80
96.31.64.0/19
AS29802
AS?
15.129.212.180
15.0.0.0/8
AS71

Sinkholing Kelihos

- Protocol was reverse engineered and encryption keys were extracted from a worker
- A special peer address for a router was propagated
- This address became the most prevalent one in the botnet, resulting in all bots talking to it
- At the same time, a specially crafted list of controller nodes was distributed



Bot Locations



What next?

- Temporary solution
- IP addresses of infected machines sent to ISP’s
- Use bot’s own update process to remove itself?
- Kelihos Botnet returns – better encryption and new techniques
- Microsoft goes after creator in Russia

Lessons Learned from Sinkholing Kelihos

- It is impossible to neutralize a botnet by taking control over the controller machines or substituting the controller list without any additional actions.
- It is still possible to push an update tool on infected machines to neutralize the botnet.
- Most effective method to disable botnet is to find the creators

References

- Garnaeva, Maria. "**Kelihos/Hlux Botnet Returns with New Techniques."** *Securelist*. 31 Jan. 2012. Web. 12 Feb. 2012. <http://www.securelist.com/en/blog/655/Kelihos_Hlux_botnet_returns_with_new_techniques>.
- Kirk, Jeremy. "**Kelihos Botnet, Once Crippled, Now Gaining Strength**." *Computerworld*. 1 Feb. 2012. Web. 12 Feb. 2012. <http://www.computerworld.com/s/article/9223885/Kelihos_botnet_once_crippled_now_gaining_strength>.
- Microsoft. **"Win32/Kelihos."** *Malware Protection Center*. Microsoft, 22 Sept. 2011. Web. 12 Feb. 2012. <http://www.microsoft.com/security/portal/Threat/Encyclopedia/Entry.aspx?Name=Win32%2fKelihos>.
- Werner, Tillmann. **"Botnet Shutdown Success Story: How Kaspersky Lab Disabled the Hlux/Kelihos Botnet."** *Securelist*. 28 Sept. 2011. Web. 12 Feb. 2012. <http://www.securelist.com/en/blog/208193137/Botnet_Shutdown_Success_Story_How_Kaspersky_Lab_Disabled_the_Hlux_Kelihos_Botnet>.