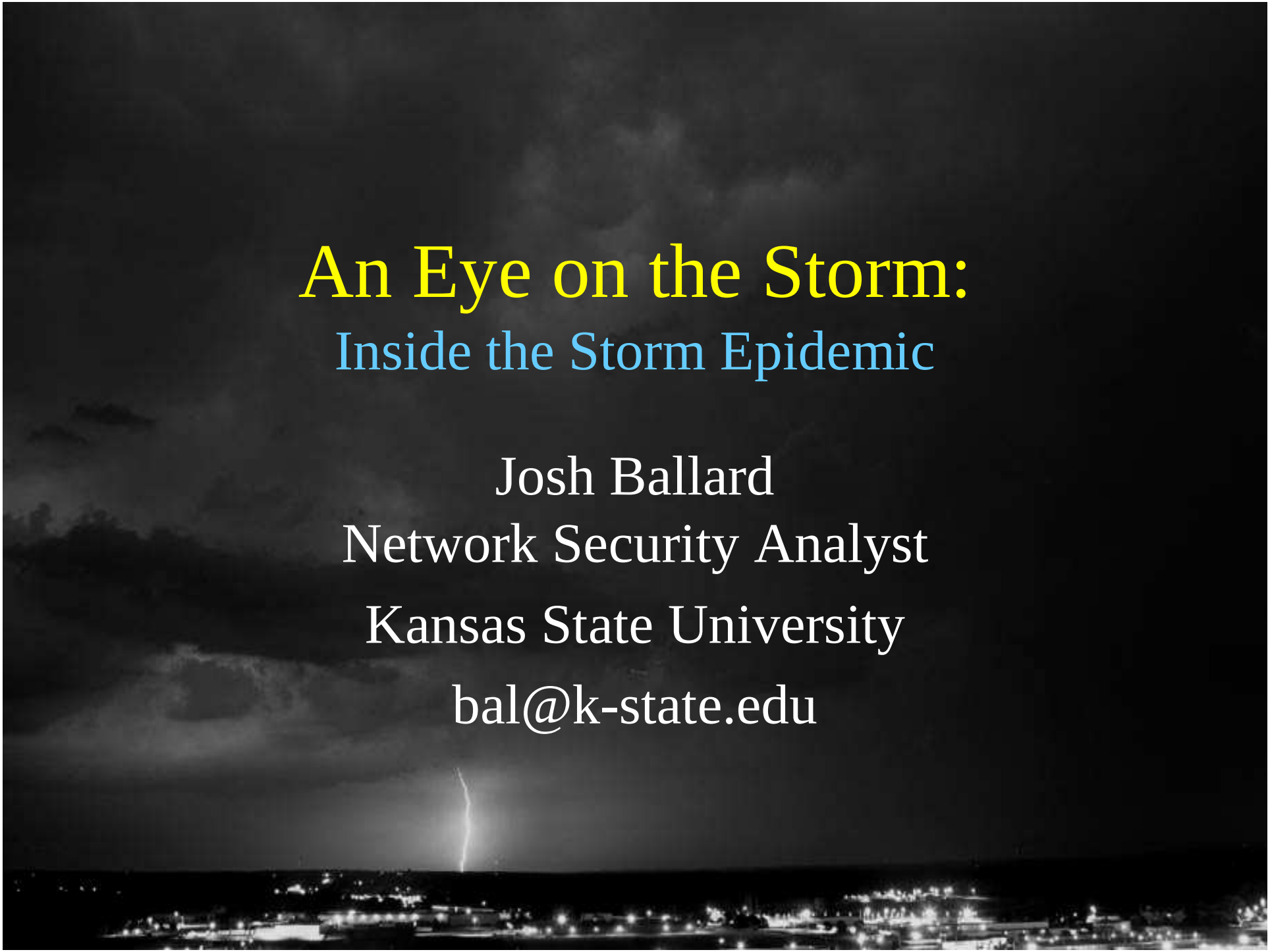
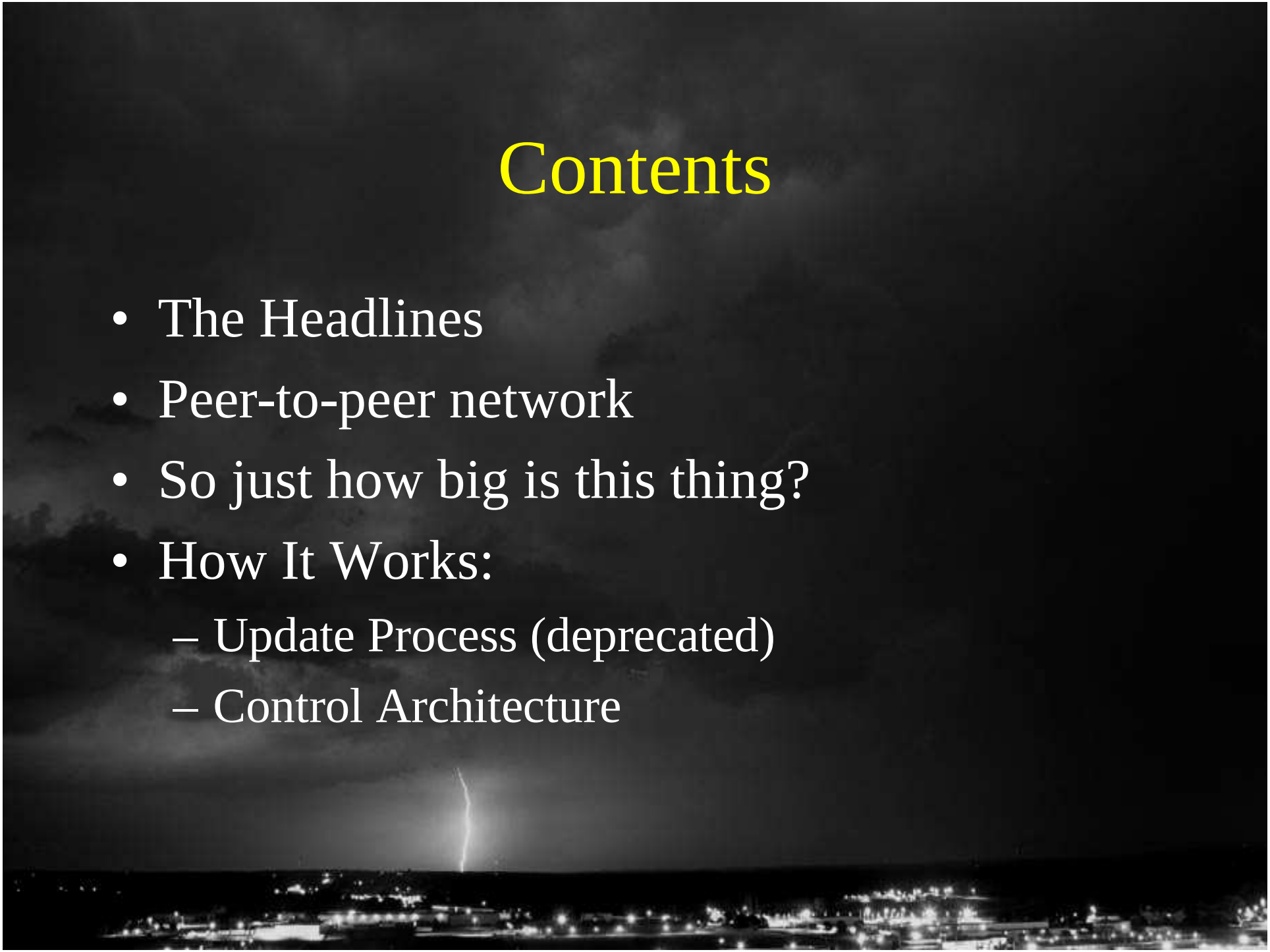


An Eye on the Storm:

Inside the Storm Epidemic

Josh Ballard
Network Security Analyst
Kansas State University
bal@k-state.edu



Contents

- The Headlines
- Peer-to-peer network
- So just how big is this thing?
- How It Works:
  - Update Process (deprecated)
  - Control Architecture

The Headlines

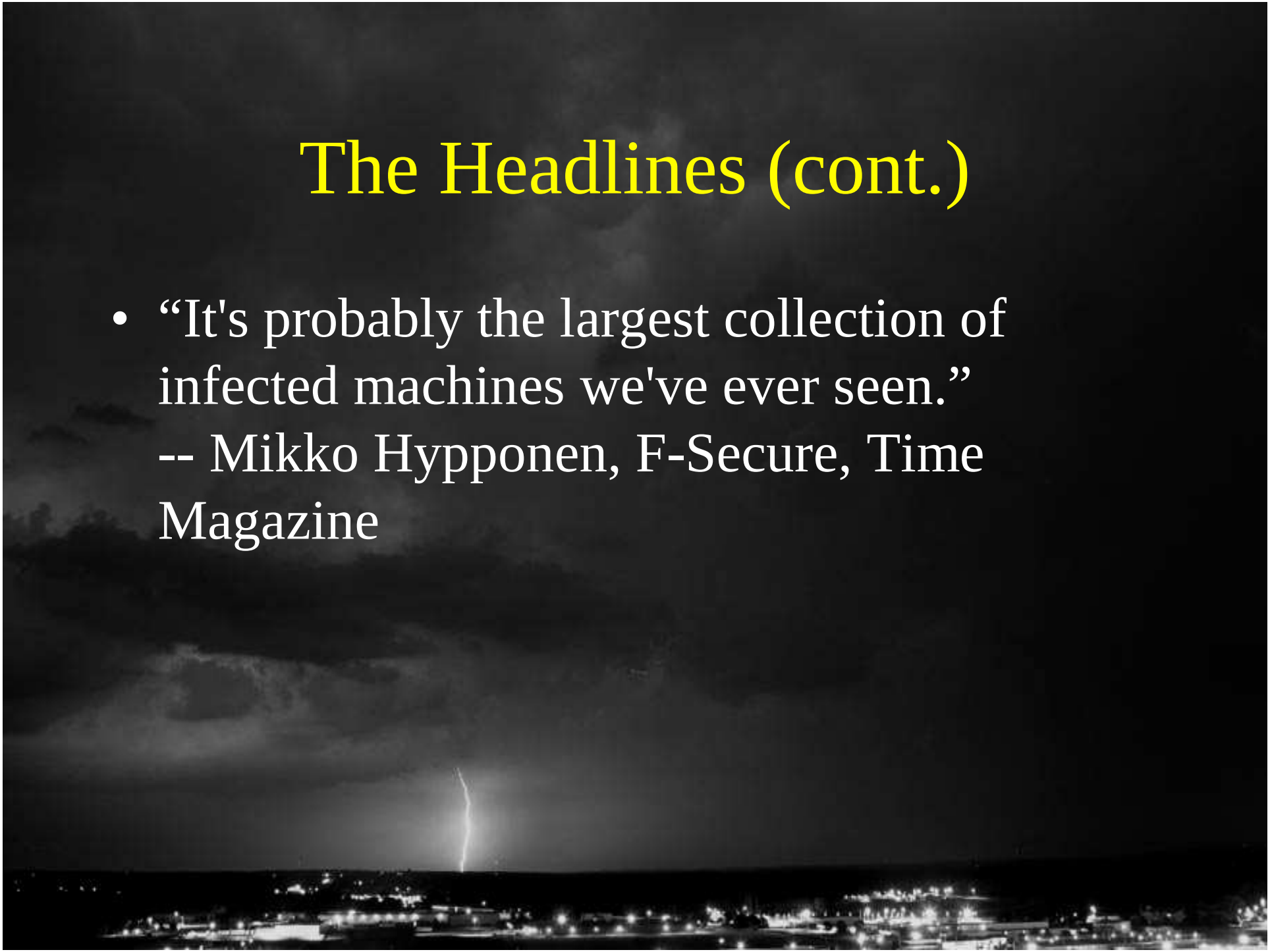
- “Bots Launching Storm Attacks Increase Dramatically Totaling 1.7 Million in June/July” -- SecureWorks, 8/2/2007
- “The Storm botnet is enormous. Reasonable guesses would put it at around 5 or 10 million machines, but nobody can be exactly sure.” -- MessageLabs 7/13/2007

The Headlines (cont.)

- "…those spikes are usually five to 10 times what we normally see," he said, noting he suspects the botnet could be as large as 50 million computers. --MessageLabs 9/6/2007
- "Storm Worm Botnet More Powerful Than Top Supercomputers" -- InformationWeek via Prof. Peter Gutmann, Univ of Auckland

The Headlines (cont.)

- “It's probably the largest collection of infected machines we've ever seen.” -- Mikko Hypponen, F-Secure, Time Magazine

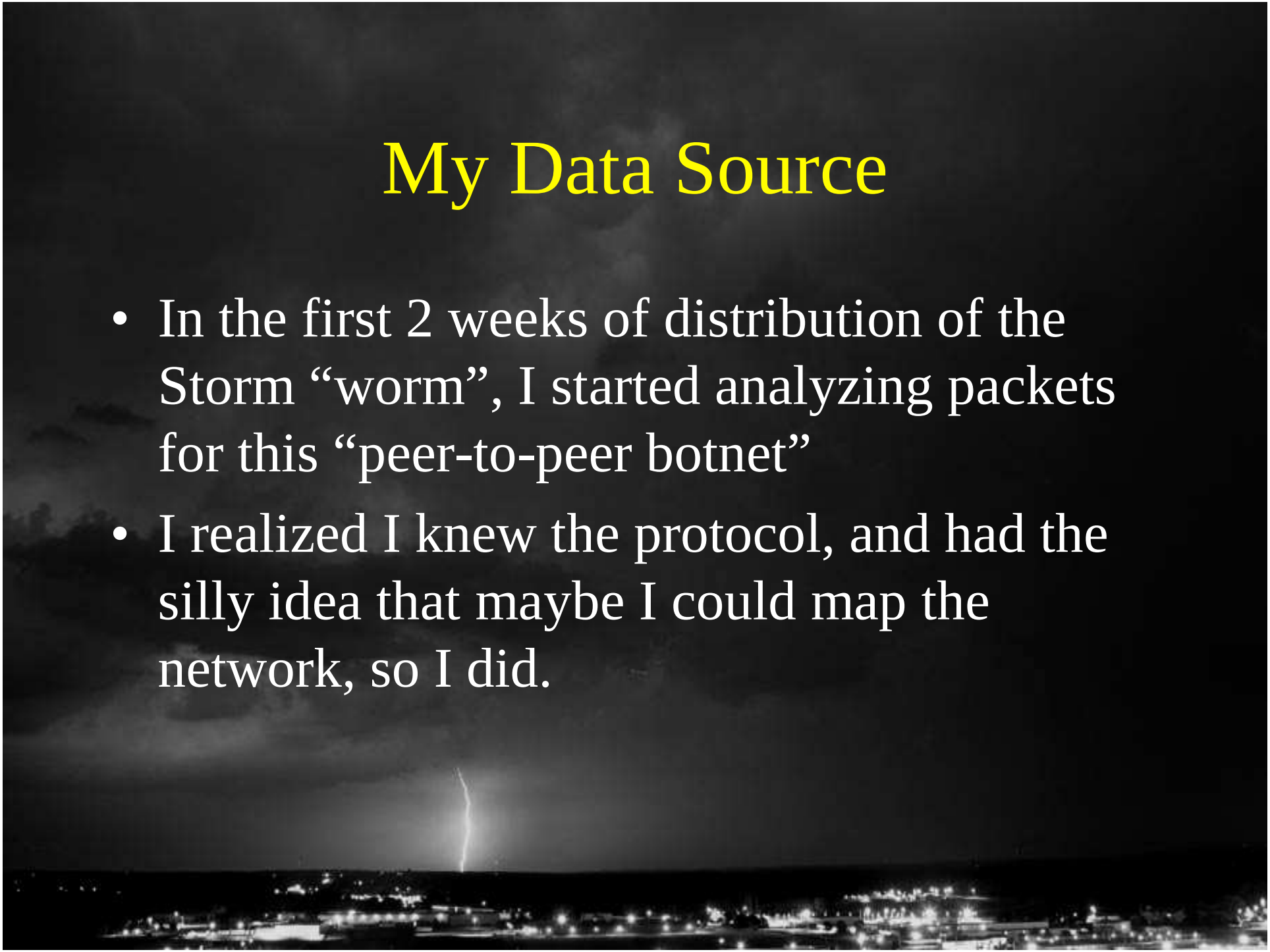


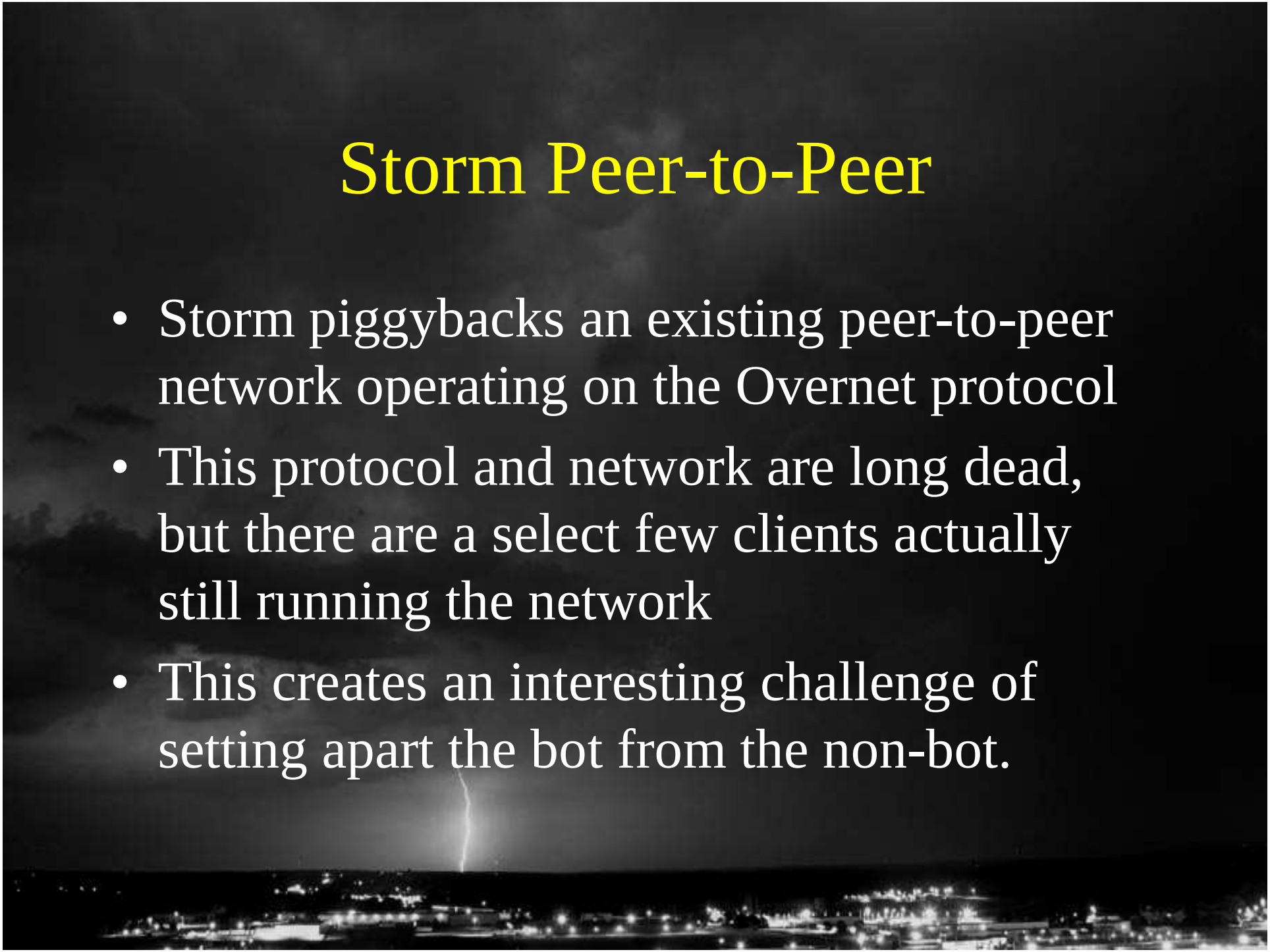
Where I’m Coming From

- I’m a protocol analyst (aka packet nerd)
- Protocol identification developer (http://hippie.oofle.com/)
- 7 years of research into protocol identification, with a heavy focus on peer-to-peer

My Data Source

- In the first 2 weeks of distribution of the Storm “worm”, I started analyzing packets for this “peer-to-peer botnet”
- I realized I knew the protocol, and had the silly idea that maybe I could map the network, so I did.





Storm Peer-to-Peer

- Storm piggybacks an existing peer-to-peer network operating on the Overnet protocol
- This protocol and network are long dead, but there are a select few clients actually still running the network
- This creates an interesting challenge of setting apart the bot from the non-bot.

Exchange Mechanism

- Client starts with a preset list of seed peers.
- Client sends a Overnet connect packet to those hosts.
- “Server” responds with an acknowledgement of peering, and a list of peers the client might be interested in, based on its hash.

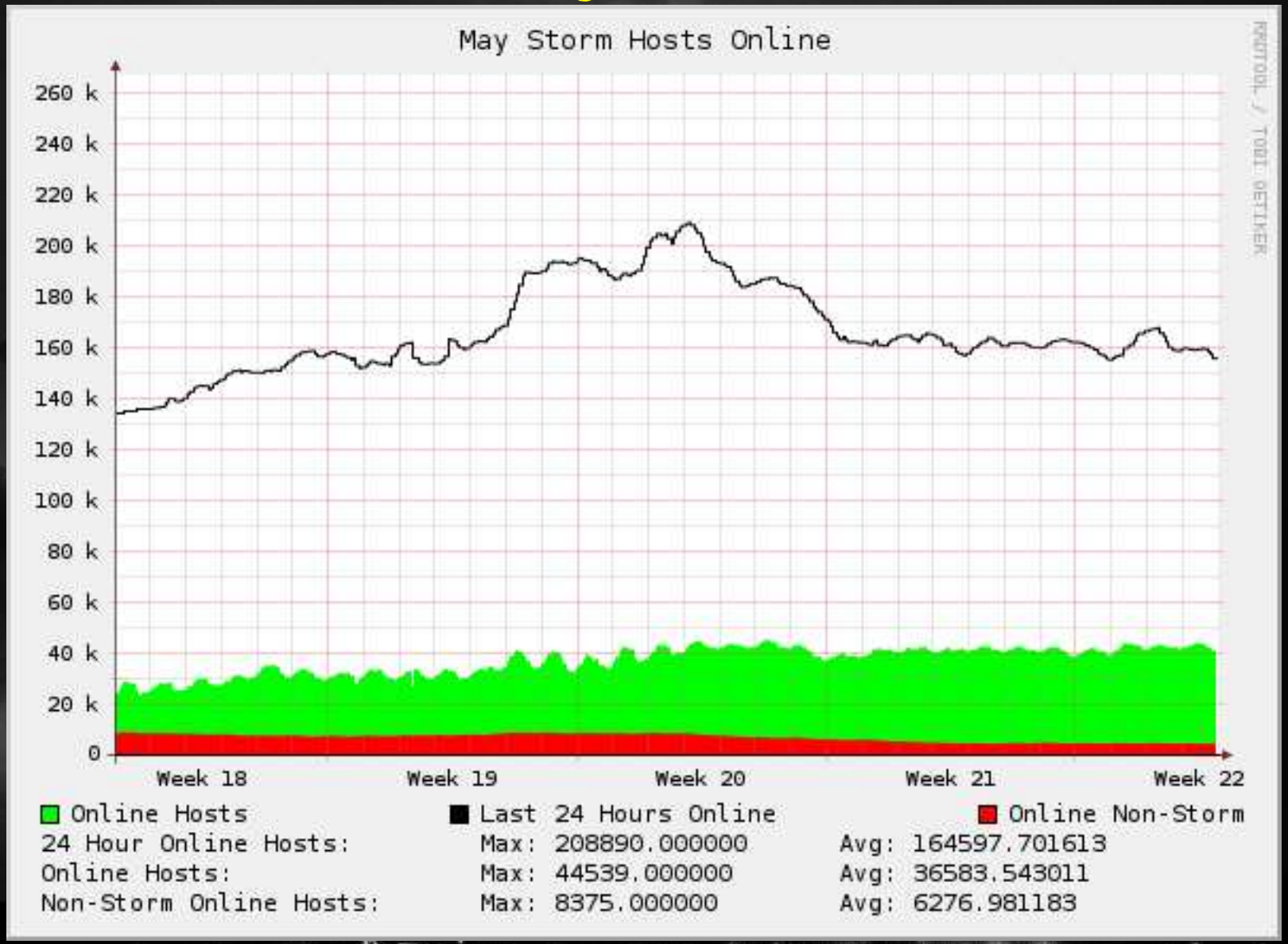
Exchange Mechanism (cont.)

- Client sends an Overnet search packet for its own hash out to the network, again soliciting more peers.
- “Server” responds with a list of peers who might be able to provide the answer to the search.
- Process is repeated until a maximum number of peering relationships are established

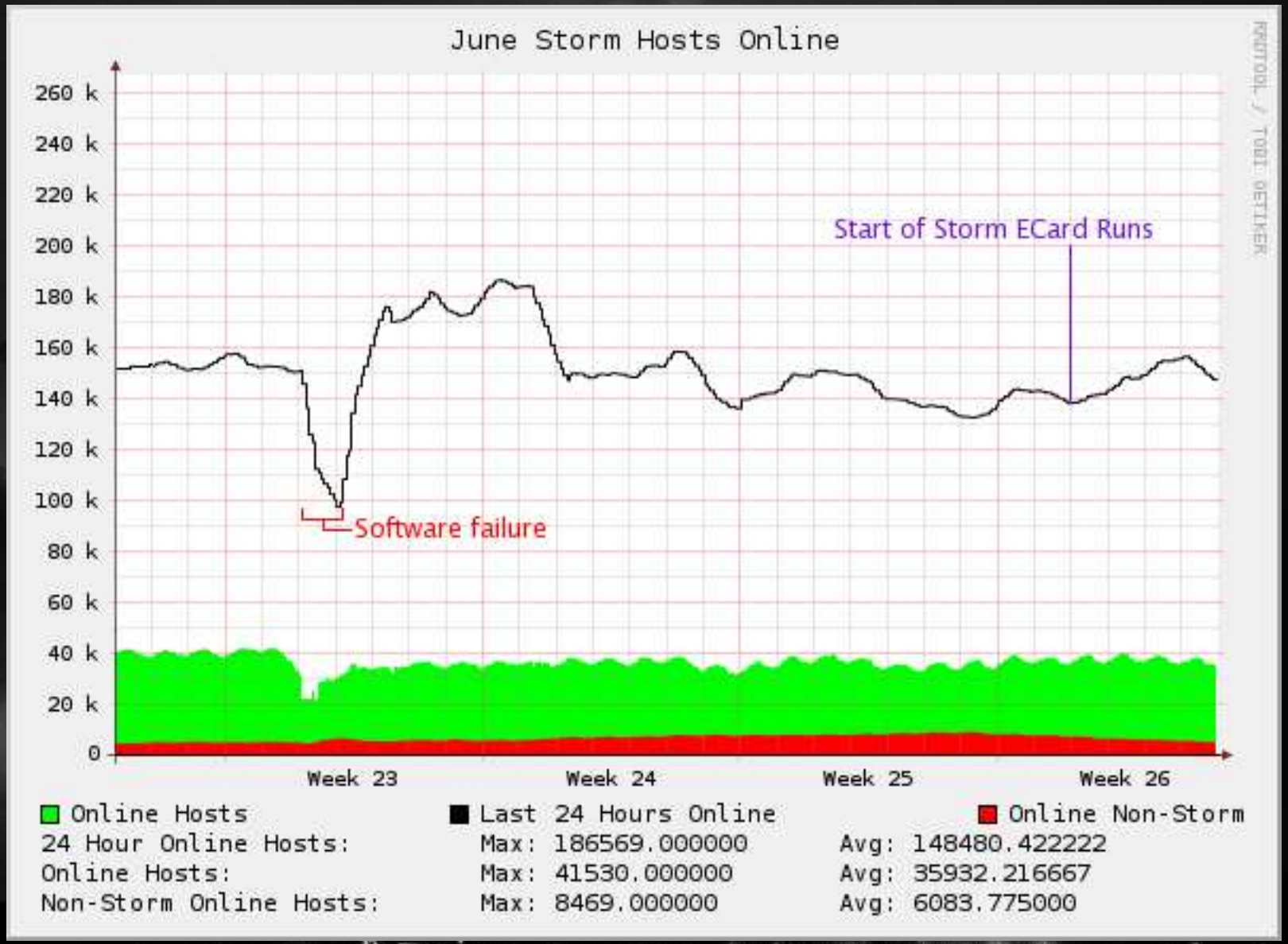
So How Big Is It?

- 11.5 million unique IP addresses since mid-April
- 6,000 average non-Storm hosts online
- 240,000 peak users in 24 hours
- 90,000 average 24 hour usage today
  - Smaller than the initial network after 1 month

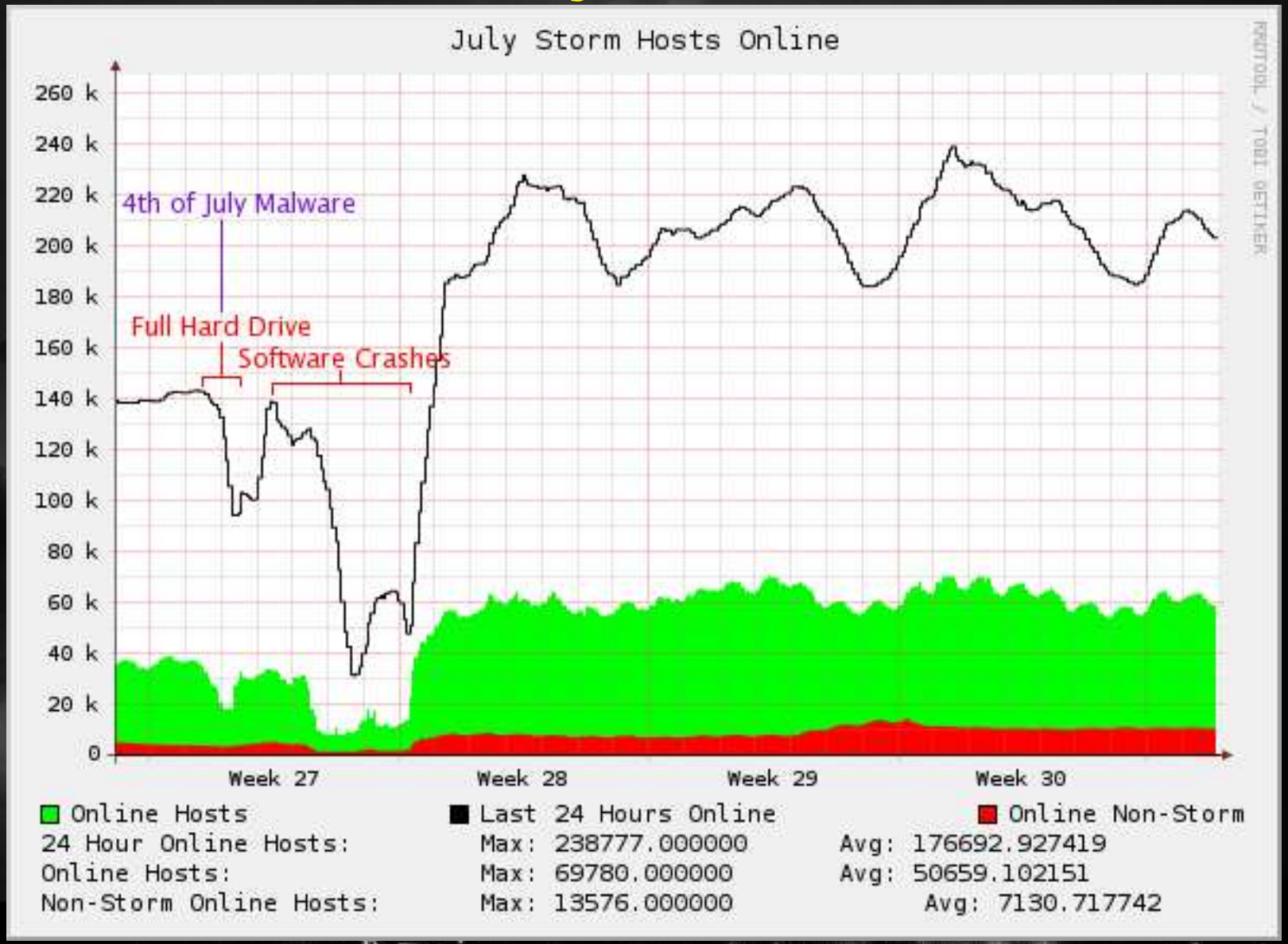
May 2007


May Storm Hosts Online
260 k
240 k
220 k
200 k
180 k
160 k
140 k
120 k
100 k
80 k
60 k
40 k
20 k
0
Week 18
Week 19
Week 20
Week 21
Week 22
Online Hosts
Last 24 Hours Online
Online Non-Storm
24 Hour Online Hosts: Max: 208890.000000 Avg: 164597.701613
Online Hosts: Max: 44539.000000 Avg: 36583.543011
Non-Storm Online Hosts: Max: 8375.000000 Avg: 6276.981183

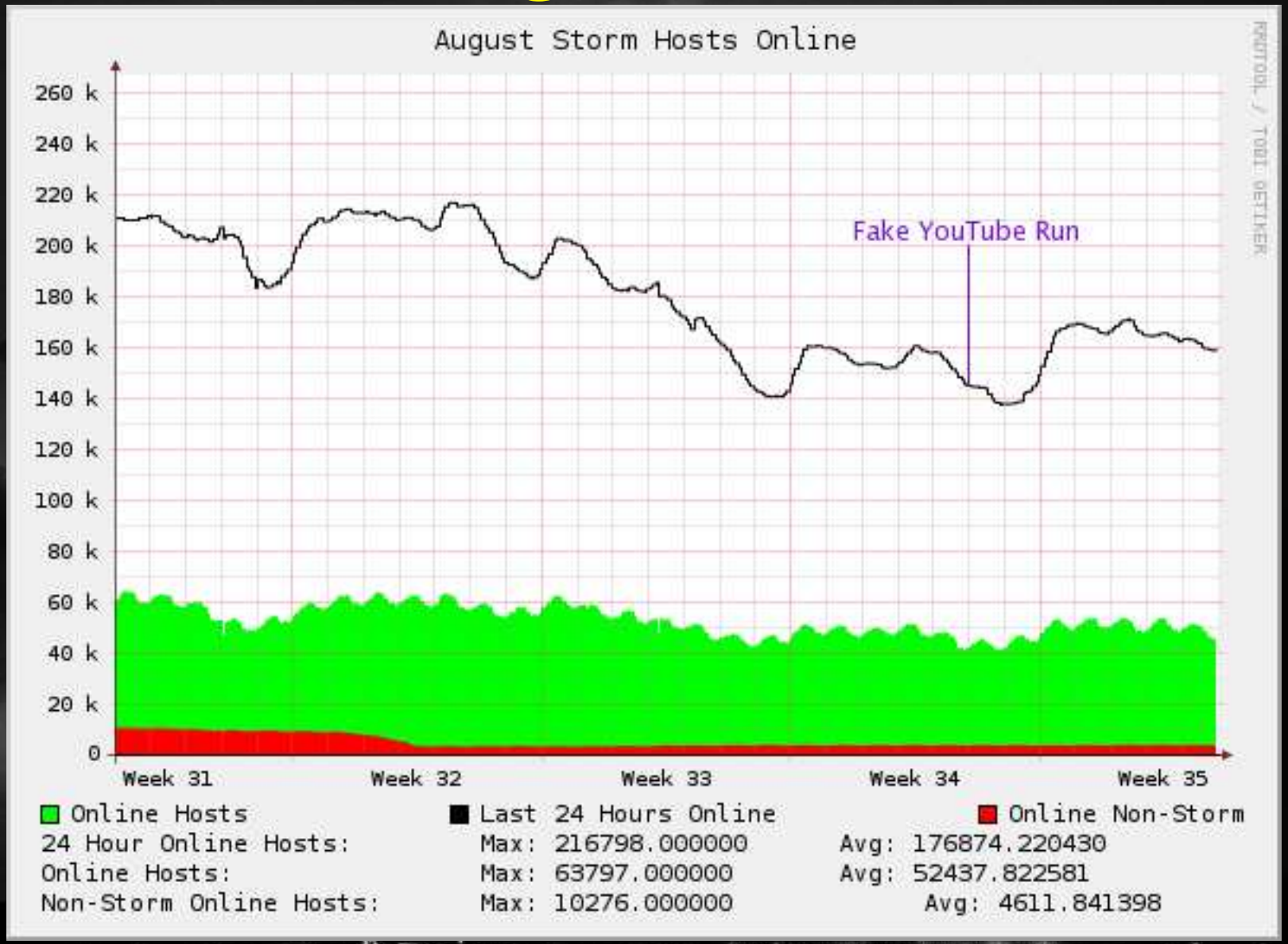
June 2007


June Storm Hosts Online
260 k
240 k
220 k
200 k
180 k
160 k
140 k
120 k
100 k
80 k
60 k
40 k
20 k
0
Start of Storm ECard Runs
Software failure
Week 23
Week 24
Week 25
Week 26
Online Hosts
Last 24 Hours Online
Online Non-Storm
24 Hour Online Hosts: Max: 186569.000000 Avg: 148480.422222
Online Hosts: Max: 41530.000000 Avg: 35932.216667
Non-Storm Online Hosts: Max: 8469.000000 Avg: 6083.775000

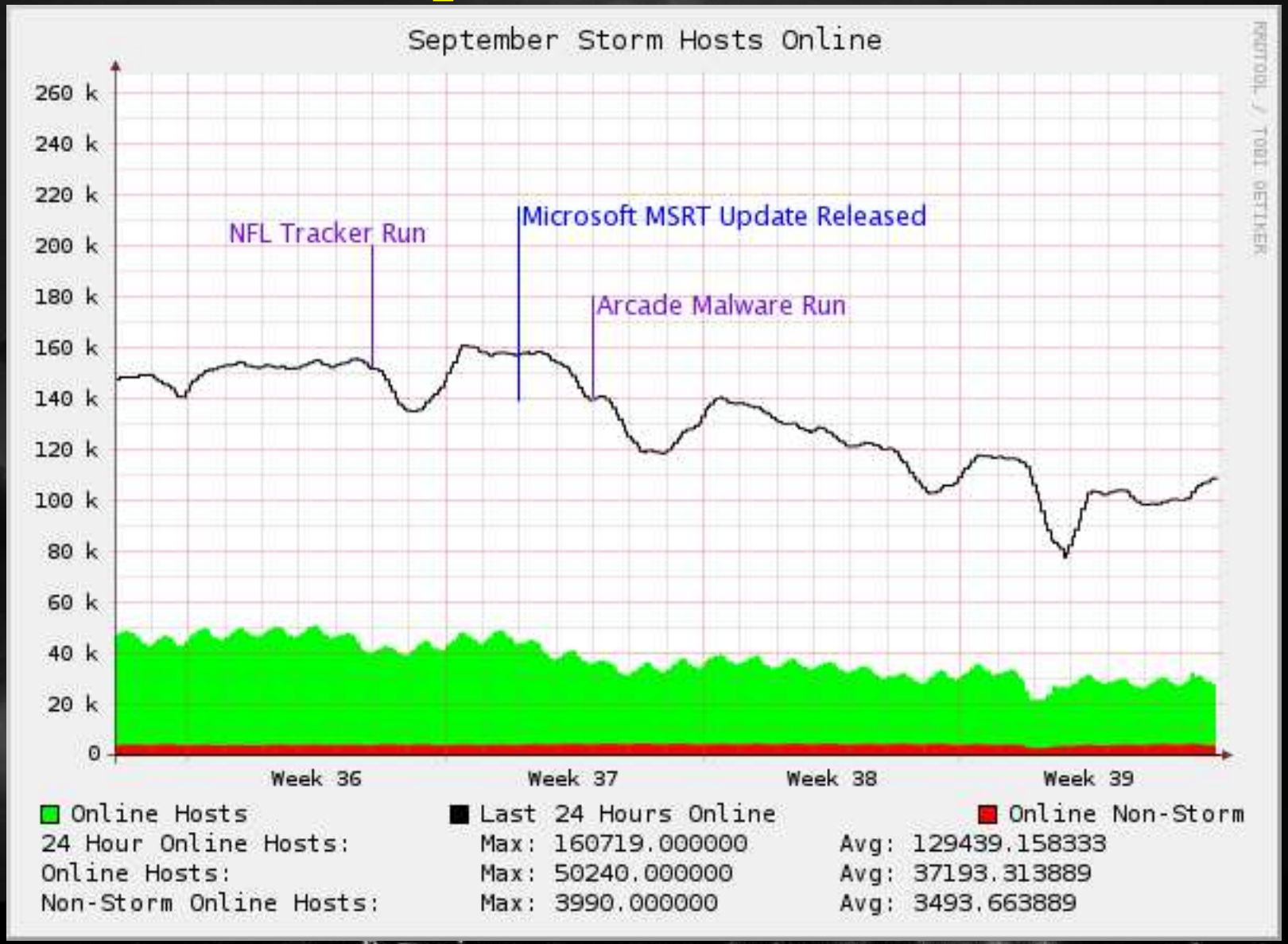
July 2007


July Storm Hosts Online
260 k
240 k
220 k
200 k
180 k
160 k
140 k
120 k
100 k
80 k
60 k
40 k
20 k
0
4th of July Malware
Full Hard Drive
Software Crashes
Week 27
Week 28
Week 29
Week 30
Online Hosts
Last 24 Hours Online
Online Non-Storm
24 Hour Online Hosts: Max: 238777.000000 Avg: 176692.927419
Online Hosts: Max: 69780.000000 Avg: 50659.102151
Non-Storm Online Hosts: Max: 13576.000000 Avg: 7130.717742

August 2007

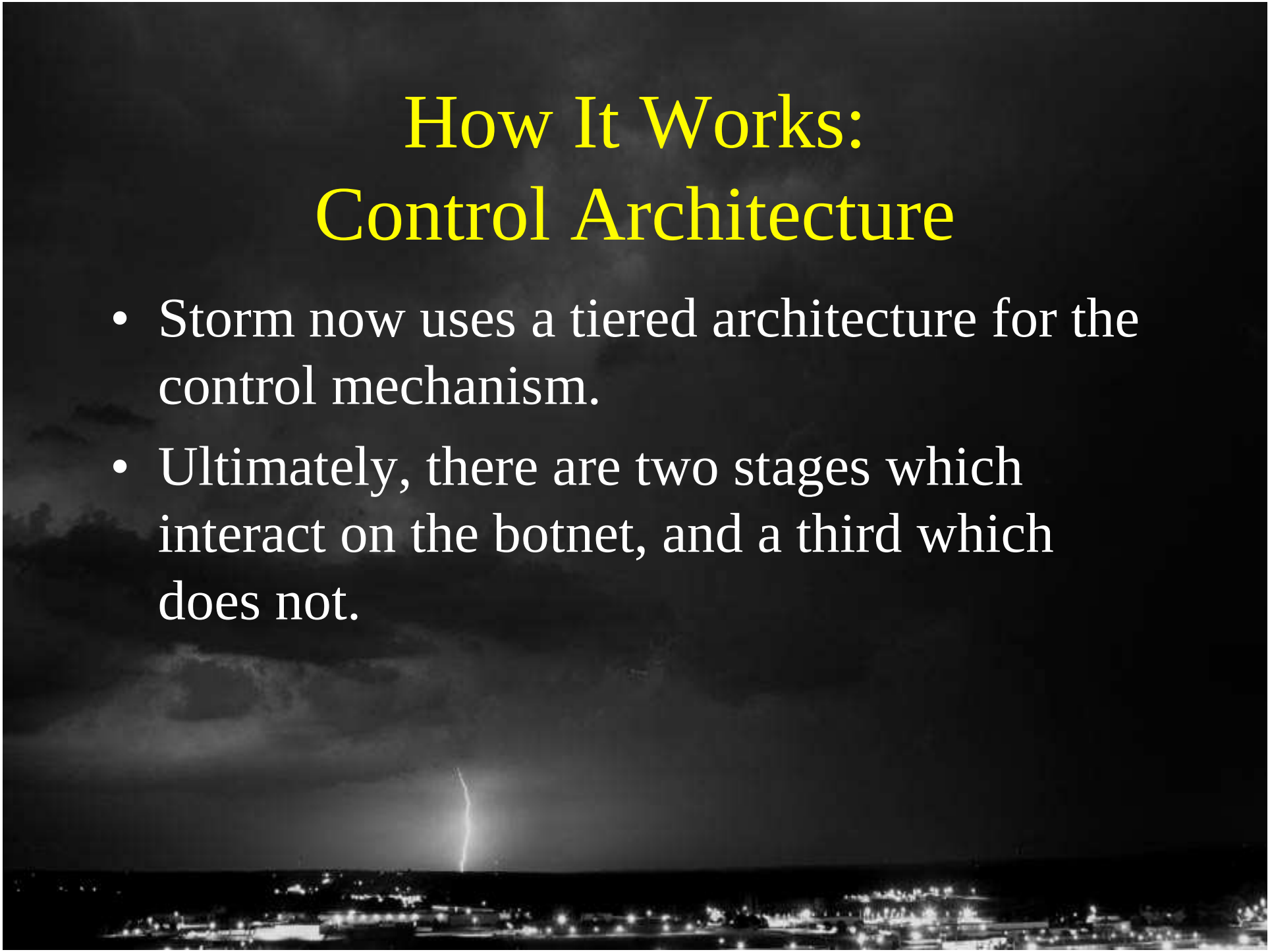

August Storm Hosts Online
260 k
240 k
220 k
200 k
180 k
160 k
140 k
120 k
100 k
80 k
60 k
40 k
20 k
0
Week 31
Week 32
Week 33
Week 34
Week 35
Fake YouTube Run
Online Hosts
24 Hour Online Hosts:
Online Hosts:
Non-Storm Online Hosts:
Last 24 Hours Online
Max: 216798.000000
Max: 63797.000000
Max: 10276.000000
Online Non-Storm
Avg: 176874.220430
Avg: 52437.822581
Avg: 4611.841398

September 2007



How It Works: Deprecated Update Process

- Once a client has reached a minimum peering point, it begins to search for updates.
- It chooses a number between 0-31, and generates a hash based on the date and that number, and begins searching for that hash.
- Controlling nodes on the network “own” those hashes for each day, and respond with update information.
- HTTP downloads ensue from encrypted URL returned.



How It Works: Control Architecture

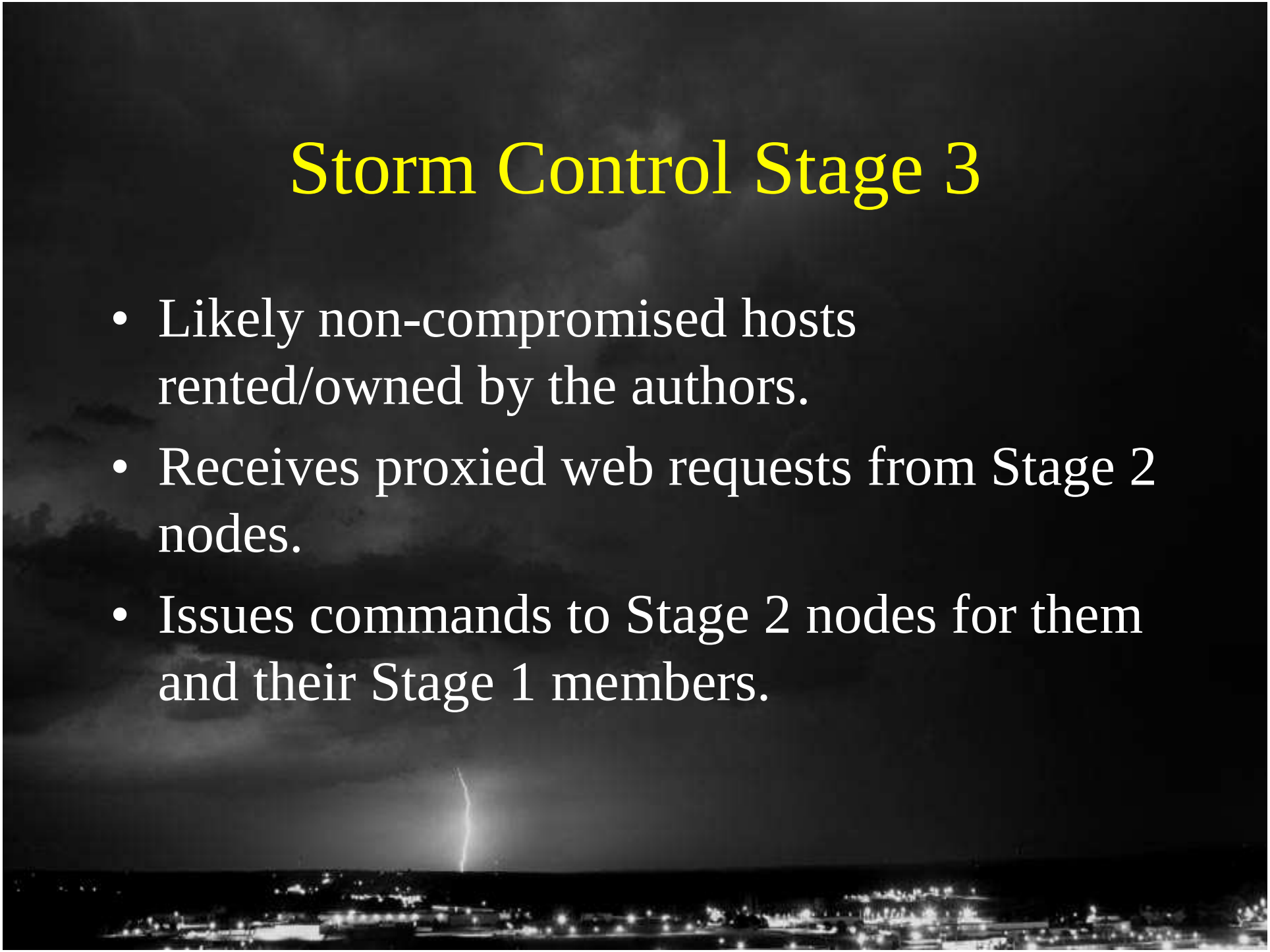
- Storm now uses a tiered architecture for the control mechanism.
- Ultimately, there are two stages which interact on the botnet, and a third which does not.

Storm Control Stage 1

- Stage 1 hosts are those which find themselves either behind a firewall (incoming connections blocked), or with RFC1918 addresses.
- This is the “attacker” stage, those hosts which carry out outbound attacks.
- These hosts are used as spam runners and DoS bots.
- Communicate up the chain to Stage 2 hosts via TCP communications.

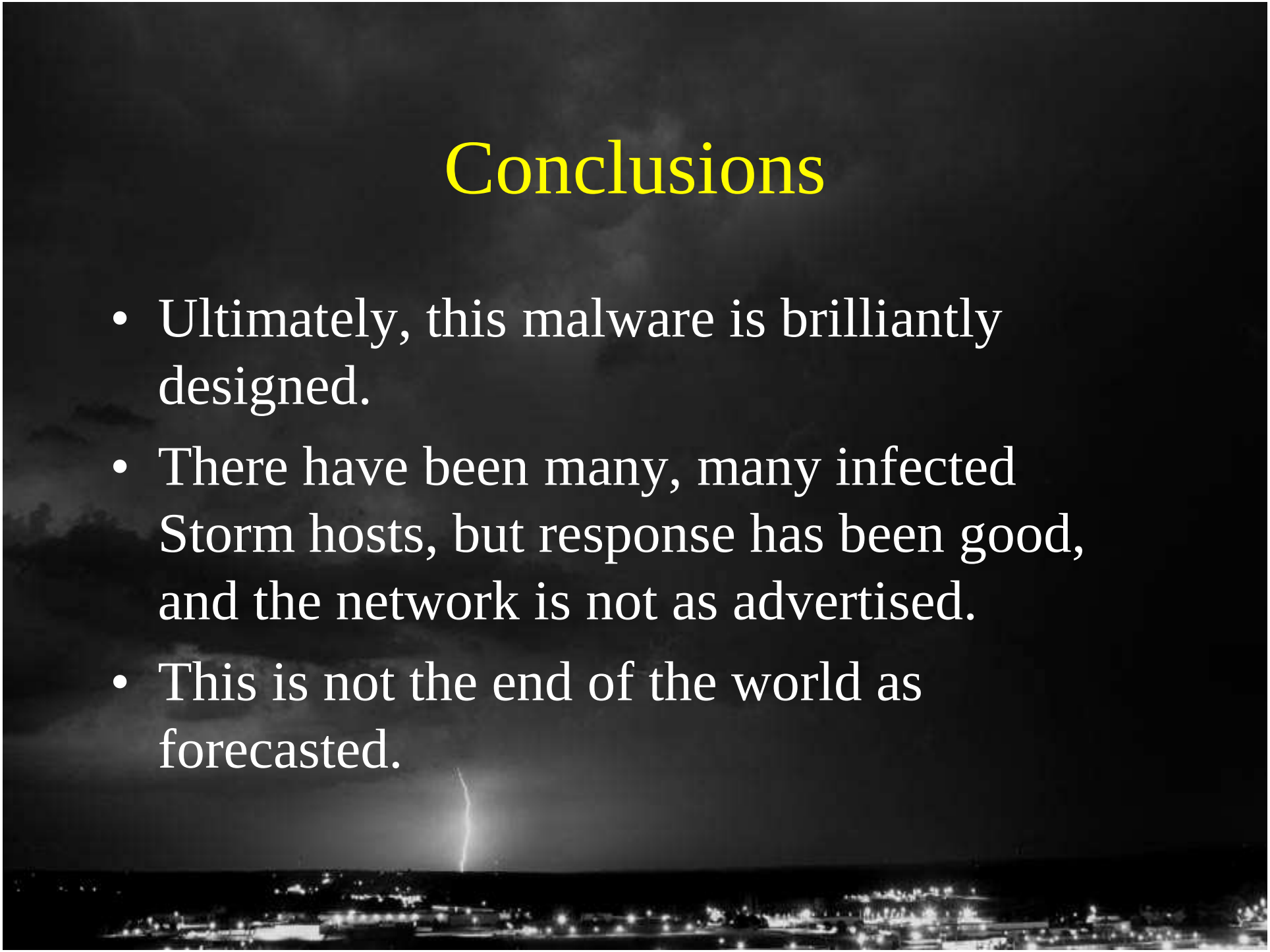
Storm Control Stage 2

- Storm Stage 2 nodes are those accessible from the outside world, but still not upper level control nodes.
- This is the “relay” or “messenger” stage of Storm.
- Stage 2 nodes will serve multiple purposes, from DNS for fast-flux domains, hosting for fast-flux, hosting for malware distribution, socks proxies, and TCP services for Stage 1 control.
- Stage 2 nodes are set to communicate to a Stage 3 control node, which is not represented on the p2p net.



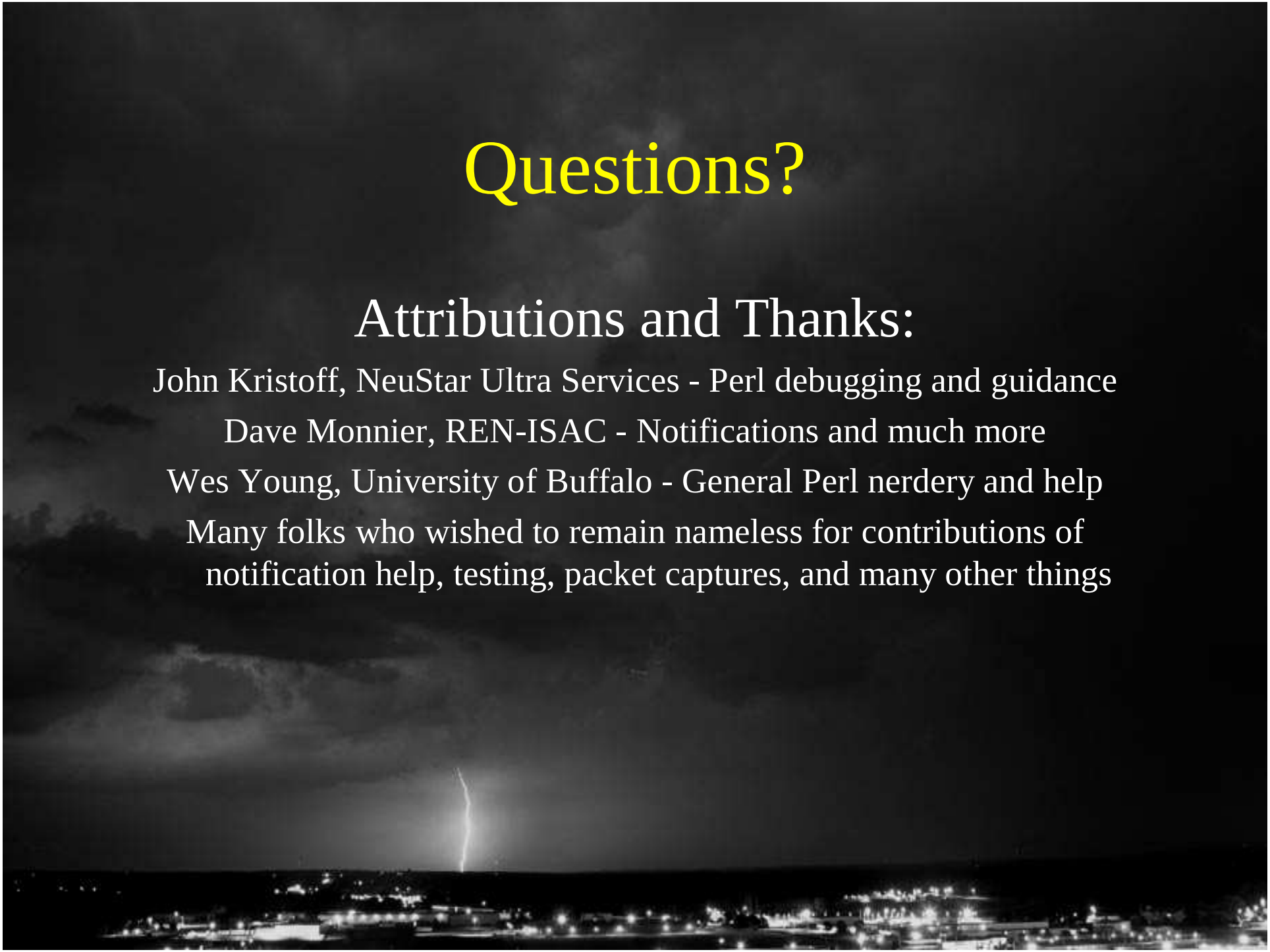
Storm Control Stage 3

- Likely non-compromised hosts rented/owned by the authors.
- Receives proxied web requests from Stage 2 nodes.
- Issues commands to Stage 2 nodes for them and their Stage 1 members.



Conclusions

- Ultimately, this malware is brilliantly designed.
- There have been many, many infected Storm hosts, but response has been good, and the network is not as advertised.
- This is not the end of the world as forecasted.



Questions?

Attributions and Thanks:

John Kristoff, NeuStar Ultra Services - Perl debugging and guidance

Dave Monnier, REN-ISAC - Notifications and much more

Wes Young, University of Buffalo - General Perl nerdery and help

Many folks who wished to remain nameless for contributions of notification help, testing, packet captures, and many other things