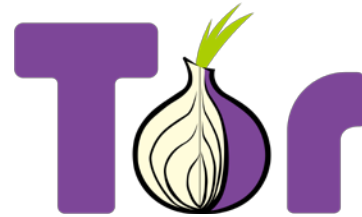


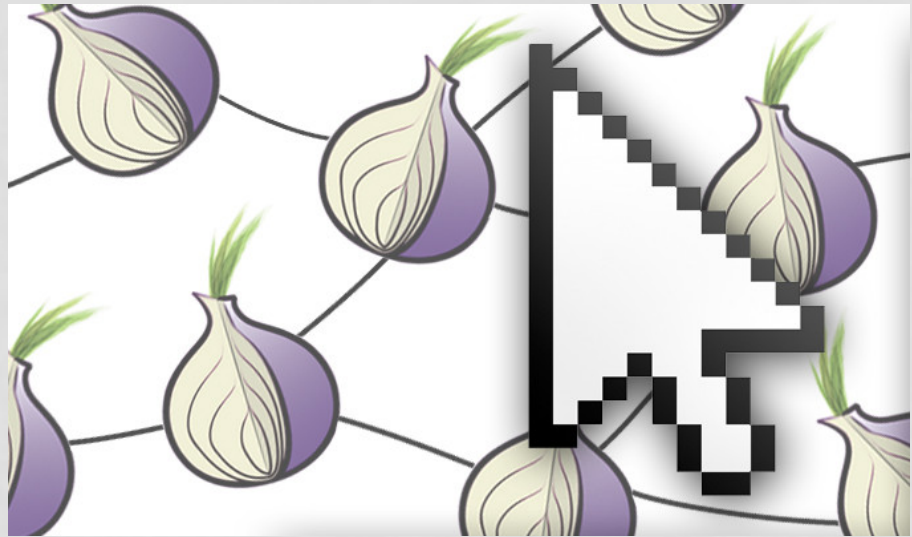
LIZARD SQUAD ATTACK ON



Andrew, Leah, Damini

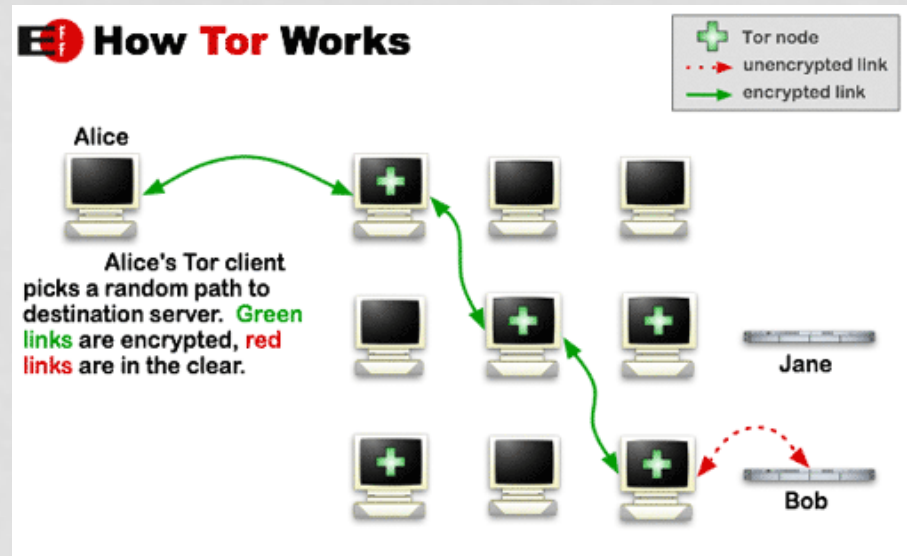
TOR

- Tor is a network of virtual tunnels.
- It allows information to be shared over public networks without compromising privacy.



HOW IT WORKS

- Data packets on the Tor network take a random pathway through several encrypted relays.
- No observer at any single point can tell where data came from or where it's going.



USES

- Tor provides a means of safe communication to whistleblowers and dissidents.
- One of the most high-profile uses of Tor was by whistleblower Edward Snowden, when he leaked classified NSA files to journalists.
- It has also been useful with “dissident movements” in Iran and Egypt.



- Although anonymity is a must for many, it also happens to be a threat to others.
- Attempts have been made in the past to try and uncover anonymity, but in vain.
- One such attempt was publicly made by the Lizard Squad



LIZARD SQUAD ATTACKS

- On December 26, 2014, the notorious hacker group Lizard Squad attempted to hack the Tor network via a DDoS attack.
- This was only a day after their successful attack on the PSN and Xbox Live networks.



Lizard Squad

@LizardMafia



To clarify, we are no longer attacking PSN or Xbox. We are testing our new Tor Oday.

12 [Follow Lizard Squad on Twitter](#)

955 RETWEETS 1,141 FAVORITES



- The Lizard Squad injected thousands of new relays in hopes of gaining a large fraction of the Tor network over a two day period.
- These new relays, however, only made up less than 1% of the Tor network by capacity.
- This resulted in short-lived attack, which ultimately failed.



- At first, their motives for this attack were quite unclear.
- The Lizard Squad expressed animosity for Tor via a tweet which stated, "Only hackers, miscreants and pedophiles use Tor."
- Nonetheless, some say it was simply a matter of prestige.
- Others fear that it was an experiment for a larger scale DDoS attack.



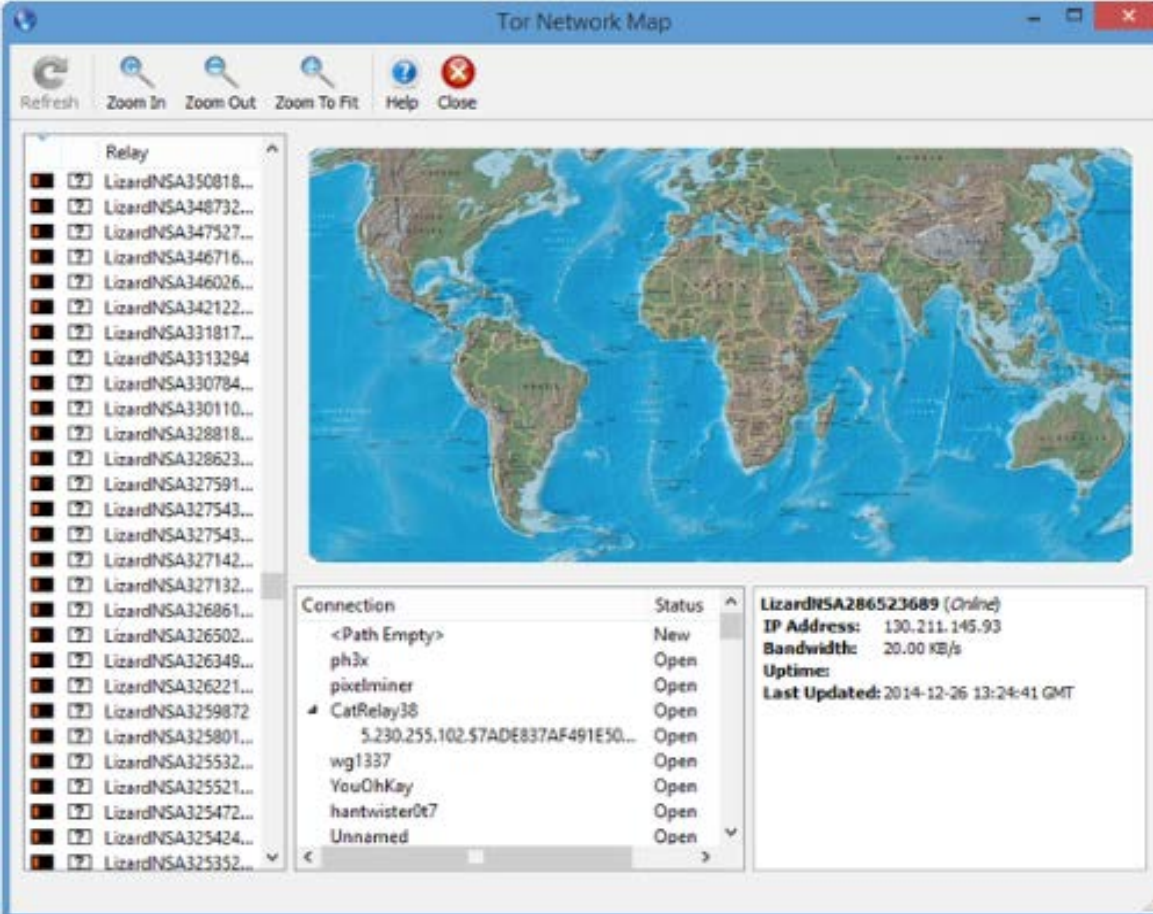
HOW THEY DID IT?

Lizard Squad added their nodes into the set of Tor nodes

How?

- Made their own nodes
- Added them to the set
- It is easy because Tor is run by volunteers, and no serious clearance check is performed.

Within an hour, Lizard Squad had 3000 new nodes added to Tor's network.



The screenshot shows the Tor Network Map application window. The title bar reads "Tor Network Map". The interface includes a toolbar with "Refresh", "Zoom In", "Zoom Out", "Zoom To Fit", "Help", and "Close" buttons. On the left, a "Relay" list displays 25 nodes, all identified as "LizardNSA" with various IDs. The main area features a world map with a network overlay. At the bottom, a "Connection" table and a detailed node information panel are visible.

Connection	Status
<Path Empty>	New
ph3x	Open
pixelminer	Open
▲ CatRelay38	Open
5.230.255.102.S7ADE837AF491E50...	Open
wg1337	Open
YouOhKey	Open
hantwister0t7	Open
Unnamed	Open

LizardNSA286523689 (Online)
IP Address: 130.211.145.93
Bandwidth: 20.00 KB/s
Uptime:
Last Updated: 2014-12-26 13:24:41 GMT



Nadim Kobeissi

@kaepora



This is what the Tor network looks like right now.

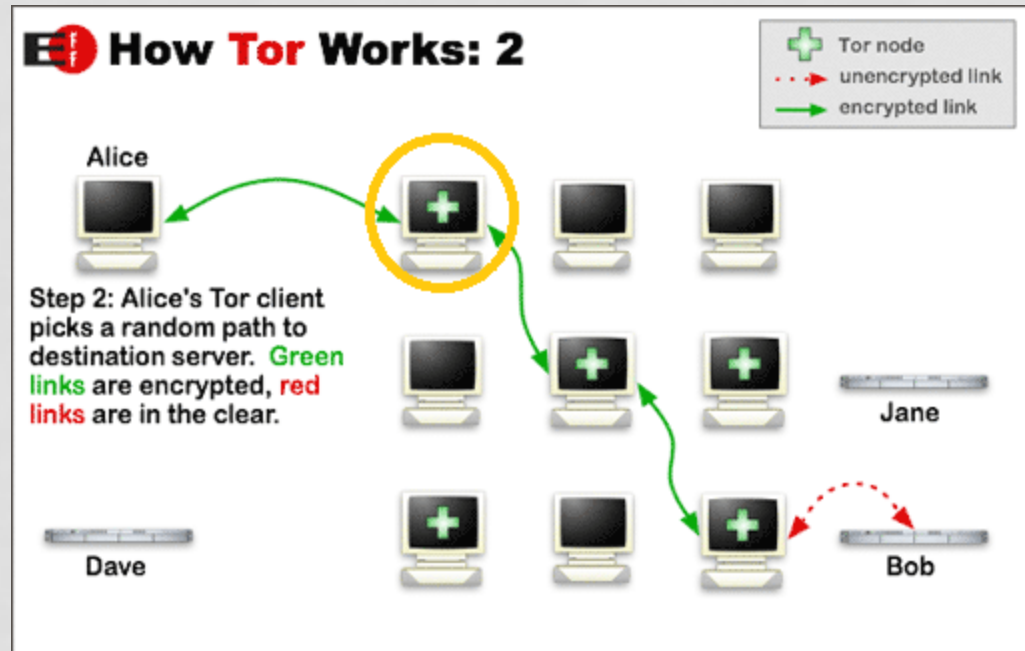
12:28 PM - 26 Dec 2014

645 RETWEETS 439 FAVORITES

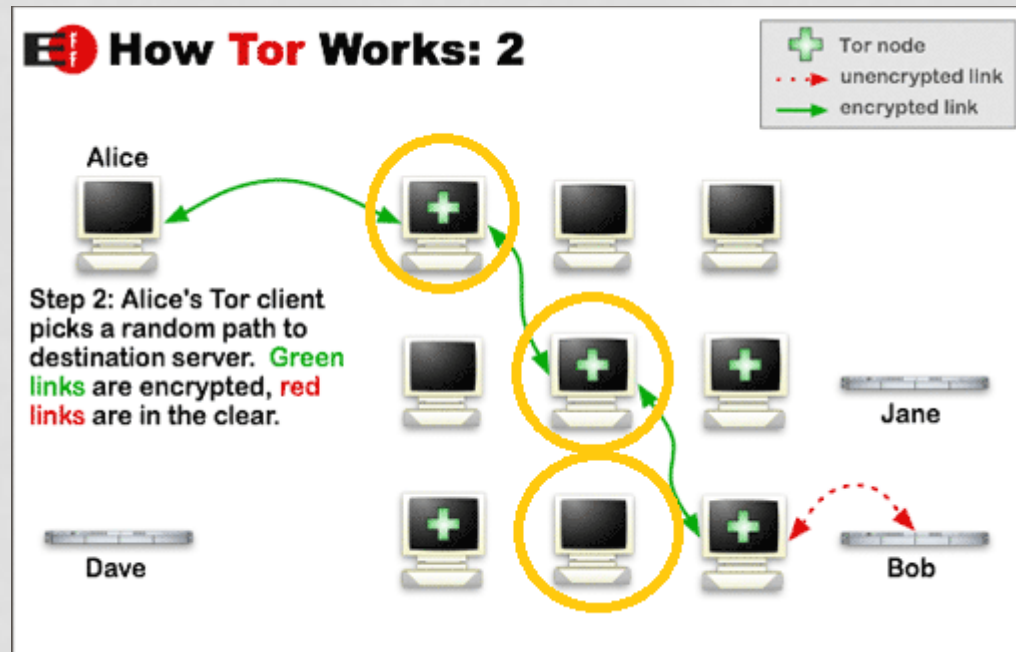


Problems

- If the random list chose only 1 node that belonged to Lizard Squad, then it would create no threat, because they would not be able to view who it came from and where it was going.

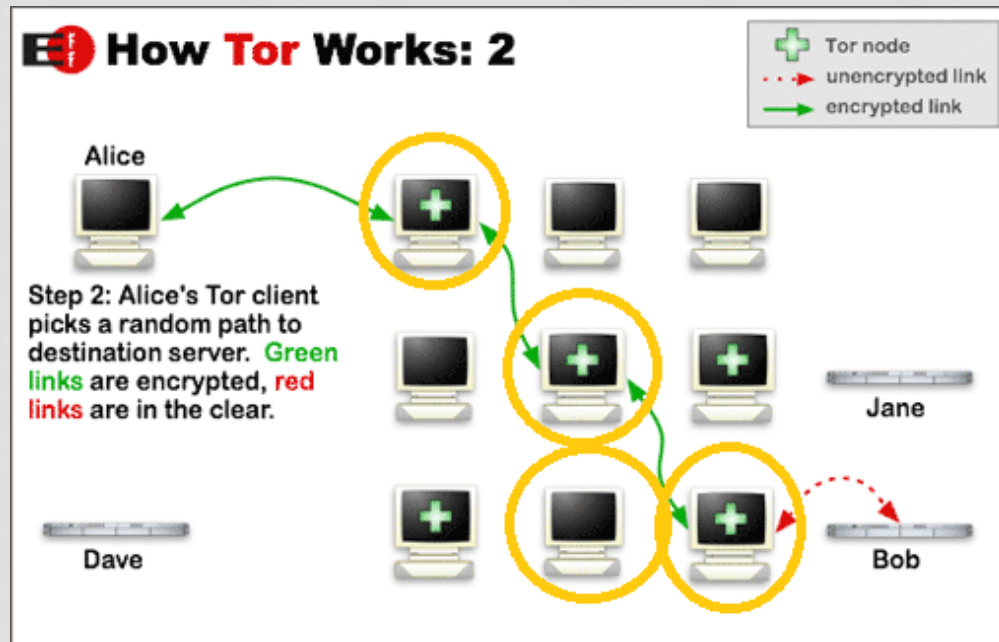


Even if Lizard Squad owned most of the nodes, it was not enough. They would still need to own all the nodes in the list to be able to connect the recipient and the sender. A few nodes in the list would be useless.

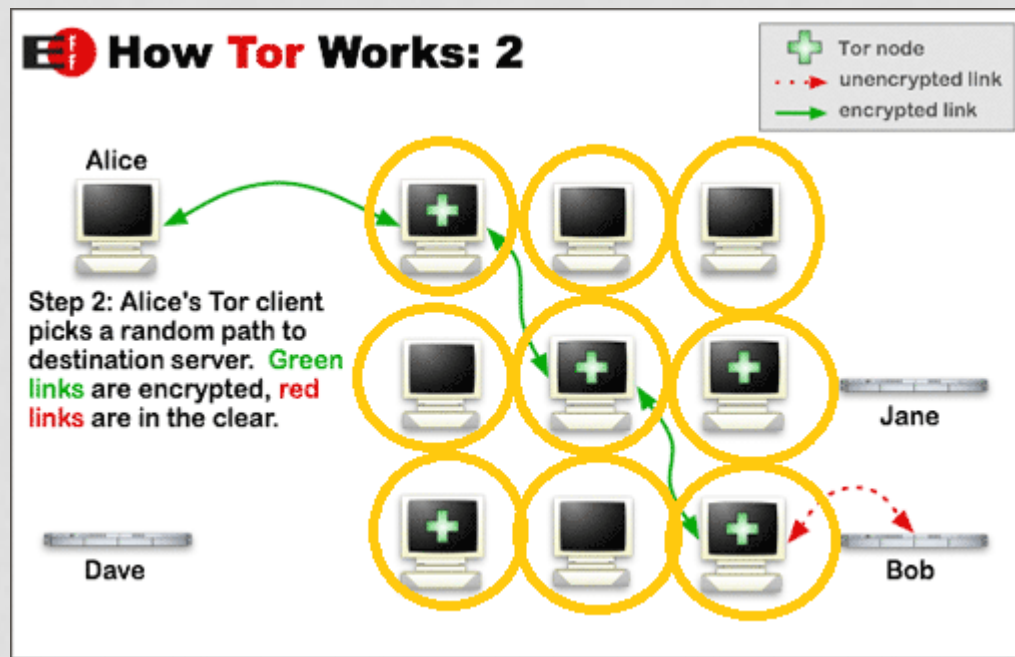


Had they been lucky enough that all the chosen nodes were owned by the Lizard Squad, then anonymity would have been endangered.

The odds of that occurring, however, was near impossible, since the amount of Lizard Squad nodes accounted for less than 1% of all the nodes.



- It would only pose a threat if they had managed to get a HUGE amount of nodes, so their nodes would add up to more than half of the nodes in the network.
- Then, the probability of the random list including all Lizard Squad nodes would be much greater, thus increasing bandwidth allowance
- And so their relays would eventually obtain consensus from the rest of the network.



WHAT TOR DID

- Detected the added nodes
- Removed the nodes from the system
- And this could have been time consuming had the number of the nodes been high, which would have put the anonymity of Tor at risk in the meantime



Not much of a threat!



- *“This looks like a regular attempt at a Sybil attack: the attackers have signed up many new relays in hopes of becoming a large fraction of the network. But even though they are running thousands of new relays, their relays currently make up less than 1% of the Tor network by capacity. We are working now to remove these relays from the network before they become a threat, and we don’t expect any anonymity or performance effects based on what we’ve seen so far.”*

ENCRYPTED CHAT INTERVIEW WITH WASHINGTON POST

- They explained that the group had control of half of the overall Tor network nodes.
- But they also acknowledged that only a very small amount of traffic was being routed through these nodes.
- The aim was to point out the structural flaws in the network.
- All the new relays had the same name so it was easily identifiable.

- There might have been ways to do this sneakily.
- Tor Project was anticipating the attack, and so had been watching out.
- Maybe one of the reasons why Lizard Squad didn't go very far with its attack on Tor was because it had been rather public.



- Lizard Squad reveals that the network is also used maliciously.



- This tweet rises suspicions and could encourage more people to try and attack the network to expose those wrongdoers

- Some believe that this attack will force the developers to strengthen the network to avoid any possible eavesdropping.
- Anonymous, an activist group of hackers supporting freedom from censorship on the Internet were outraged.
- Soon after Lizard Squad had publicly announced its intentions, Anonymous demanded that they stop.





Anonymous
@YourAnonNews

Follow

Hey @LizardMafia don't fuck with the Tor network. People need that service because of corrupt governments. Stand the fuck down.



RETWEETS

1,569

FAVORITES

2,053



But their response was



Liz Jong Un
@LizardMafia

Follow

Do something. [@YourAnonNews](#)

8:26 PM - 26 Dec 2014

571 RETWEETS 847 FAVORITES



And so they did!



Anonymous
@TheAnonMovement

[+ Follow](#)

Time to tame these Lizards? #Lulz
#OpLizardSquad #LizardSquad #Anonymous
@YourAnonNews @YourAnonGlobal

👤 Anonymous 🍏, Anonymous Press, Anonymous and 4 others



RETWEETS
916

FAVORITES
1,093



6:13 PM - 26 Dec 2014

- They tracked down members
- Later they tweeted a screenshot of an alleged conversation with a lizard member
- Joining forces with another group, they released personal details about that member of the Lizard Squad.
- Despite having been doxed by the two groups, it seems that Lizard Squad is not ready to disappear yet.

The lizards may not be attacking Tor anymore, but this wasn't the only attempt to attack the network, and it certainly won't be the last!



QUESTIONS:

How does Tor keep anonymity?

Data packets on the Tor network take a random pathway through several encrypted relays from the client to destination sever.

Why was Lizard's attempt unsuccessful?

Lizard's relays only made up 1% of the network, which is not enough to get consensus from the rest of the network. This does not affect anonymity.

How did they handle the attack?

They had been monitoring the network and once they noticed the new relays, they got started on effectively removing them.

THANK YOU

REFERENCES:

1. <http://www.businessinsider.com/anonymous-to-lizard-squad-stop-attacking-tor-2014-12>
2. <http://betanews.com/2014/12/27/lizard-squad-attacks-tor-network-ignoring-warning-from-anonymous/>
3. <http://news.softpedia.com/news/Lizard-Squad-s-Attack-On-Tor-Anonymity-Network-Adds-3-000-New-Relays-468391.shtml>
4. <http://betanews.com/2014/12/26/anonymous-declares-war-on-lizard-squad-after-ddos-attacks-on-game-networks/>
5. <http://www.washingtonpost.com/blogs/the-switch/wp/2014/12/26/the-hackers-who-say-they-took-down-gaming-networks-are-now-going-after-tor/>
6. http://www.reddit.com/r/technology/comments/2qmp99/tor_might_be_compromised_hacker_group_lizard/
7. <http://thehackernews.com/2014/12/Lizard-Squad-Xbox-playstation.html>
8. <http://www.techtimes.com/articles/23334/20150101/tor-attack-pits-anonymous-against-lizard-squad-psn-and-xbox-live-recovering.htm>
9. <http://www.neowin.net/news/anonymous-goes-after-lizard-squad-for-attacking-the-anonymity-network-tor>
10. <http://www.zdnet.com/article/tor-not-at-risk-after-failed-attack-by-lizard-squad-hackers/>
11. <http://www.businessinsider.com.au/anonymous-to-lizard-squad-stop-attacking-tor-2014-12>
12. <http://anonhq.com/lizard-squad-attacks-tor-falls-flat-face/>
13. <https://www.torproject.org/about/overview.html.en>
14. <http://www.zdnet.com/article/tor-not-at-risk-after-failed-attack-by-lizard-squad-hackers/>
15. <http://anonhq.com/lizard-squad-attacks-tor-falls-flat-face/>
16. <https://www.torproject.org/about/overview.html.en>
17. <http://www.zdnet.com/article/tor-not-at-risk-after-failed-attack-by-lizard-squad-hackers/>