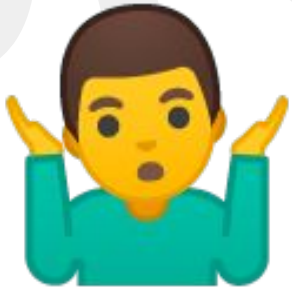
Abuse Deep-Dive: DDoS and Botnets

IETF PEARG Research Group Interim Meeting, 2021-01-19

what's wrong with a little abuse?



25 The Democratization of Censorship

SEP 16

John Gilmore, an American entrepreneur and civil libertarian, once famously quipped that "the Internet interprets censorship as damage and routes around it." This notion undoubtedly rings true for those who see national governments as the principal threats to free speech.

However, events of the past week have convinced me that one of the fastest-growing censorship threats on the Internet today comes not from nation-states, but from super-empowered individuals who have been quietly building extremely potent cyber weapons with transnational reach.

All About Skimmers

National Security

Banks seek NSA help amid attacks on their computer systems

U.S. Bancorp website targeted by purported Middle East group

January 11, 2013

Major U.S. banks ha
after a barrage of as

The attacks on the s
increasingly sophist
asked to provide tec

Chase joins Bank of America in possible Islamic attack outage

Another target of the 'Cyber fighters of Izz ad-din Al qassam'?

BB&T
October 17, 2012 ·

BBT.com is experiencing intermittent delays and outages. We apologize for the inconvenience and assure you that your accounts and personal information remain secure. Please know that we are working diligently to restore service as soon as possible.

Customers reporting BofA website problems

The cooperation between the NSA and banks, industry officials say, underscores the government's fears

part
the a
vate

strict purpose of improving computer security.

Critical Infrastructure … National Security?

Capital One Targeted Again in Cyber Attack Spree

Response latency

Attacks lead to immediate outages, and therefore need immediate attention

Humans are slow… typical time to triage an issue and take action is 20 minutes

→ Automation is key, looking at behavior over seconds or minutes, not hours or days

How can we identify/filter bad traffic?

Identification

Find characteristics of the abusive traffic that are rarely present in legitimate traffic.

- request
- user-agent
- referer
- request rate
- ....

Filtering

Block the attack in a way they can't easily bypass by modifying the attack.

- UDP amplification attacks can often be blocked by source port
- TCP amplification attacks can be blocked by filtering SYN-ACK packets to servers that don't make outbound connections
- Otherwise… need to rely on IP filtering (and hope it's not spoofed!)

Collateral Damage

What happens when multiple users share an IP?

- Good for privacy (it's slightly harder for a website to distinguish between them, though still possible through cookies or other identifying characteristics).
- Introduces significant collateral damage to any IP-based blocking.
- CAPTCHAs reduce the harm, but annoy users.

TC

Large DDoS attacks cause outages at Twitter, Spotify, and other sites

Darrell Etherington, Kate Conger

/ 5:31 AM PDT • October 21, 2016

WIRED BACKCHANNEL BUSINESS CULTURE MORE SIGN IN SUBSCRIBE

LILY HAY NEWMAN SECURITY 10.21.2016 01:04 PM

What We Know About Friday's Massive East Coast Internet Outage

DNS service Dyn faces DDoS attacks.

THE VERGE TECH SCIENCE ENTERTAINMENT MORE

WEB REPORT US & WORLD

117

How an army of vulnerable gadgets took down the web today

Malware known as Mirai is targeting the smart home

By Nick Statt | @nickstatt | Oct 21, 2016, 4:55pm EDT

Source Brian Krebs (Twitter) | Via Wired

After Dyn cyberattack, lawmakers seek best path forward

(From left to right) Level 3 Communications' chief security officer Dale Drew, computer security luminary Bruce Schneier and niversity of Michigan's Dr. Kevin Fu / Credit: C-Span video

Hacking

Massive cyber-attack grinds Liberia's internet to a halt

The attack was a distributed denial of service, in which a network of infected computers is directed to bombard its target with traffic and overload its servers

Nicky Woolf *in San Francisco*

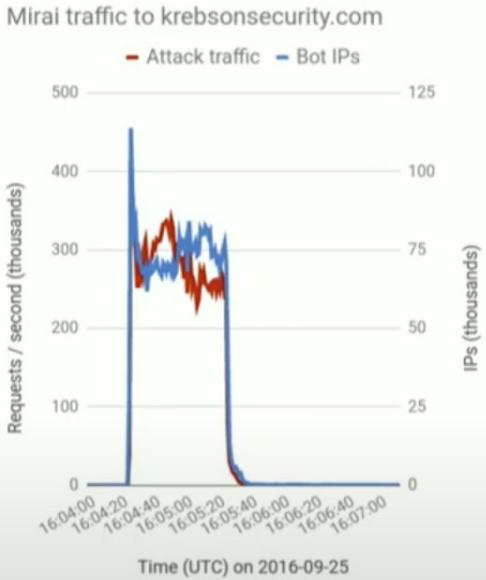
@nickywoolf

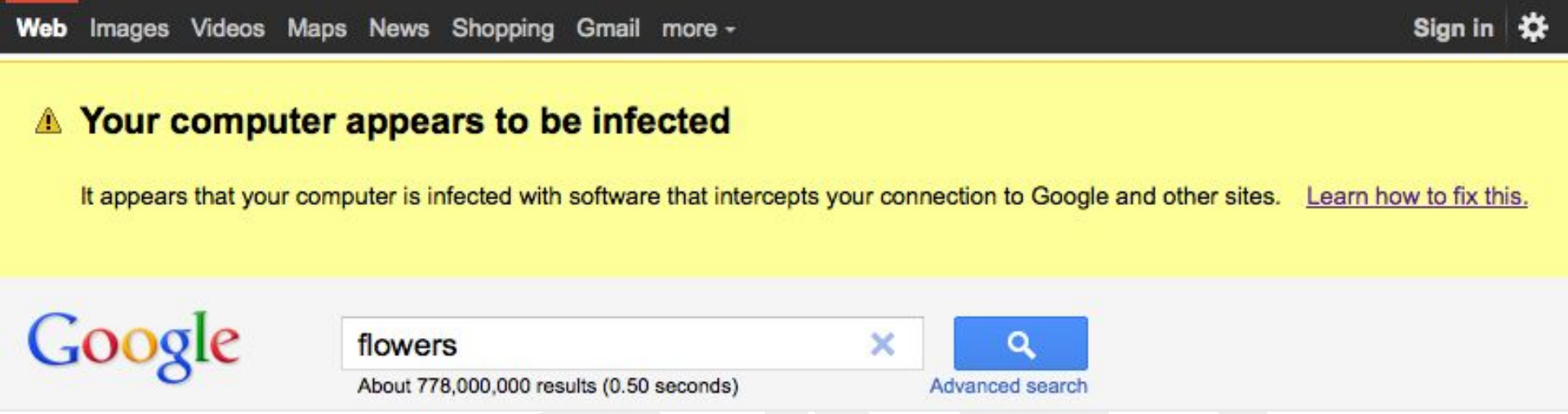
Thu 3 Nov 2016 15.15 EDT

The entire internet infrastructure of the African nation of Liberia has been brought to a grinding halt after it was targeted by hackers using the same

Investigation

- On September 25th, krebsonsecurity.com, now hosted via Google Project Shield, was attacked by Mirai.
- Alaskan IPs (devices) participated in the attack.
- Brian Krebs authorized Google to share attack data with FBI Anchorage.
- Ultimately, Jha, White, and Norman would be searched and interviewed by FBI and partners.
- One by one they agreed to cooperate and plea…
- FBI Chicago and San Diego dismantled Remaiten.





Subject: DDoS from your IPs to Google

We observed machines under your control participating in a DDoS attack targeting Google IPs. The machines are not owned by malicious customers, but rather have been compromised by the XOR.DDoS botnet, possibly due to weak passwords.

"Social Good"

We're all here because we believe Privacy is important.

But… solutions need to consider tradeoffs including:

- censorship
- threats to critical infrastructure and national security
- threats to the stability of the internet itself
- ability to investigate botnets
- ability to notify users their machines have been compromised
    - **there is no privacy without security!**