Changes observed during the COVID-19 and the Lockdown. Some data related to the ITU Africa region.

Regional Dialogue for Africa (AFR)

Securing Critical National Infrastructure

23 September 2020

www.bitsight.com

Background and Cybersecurity Trends

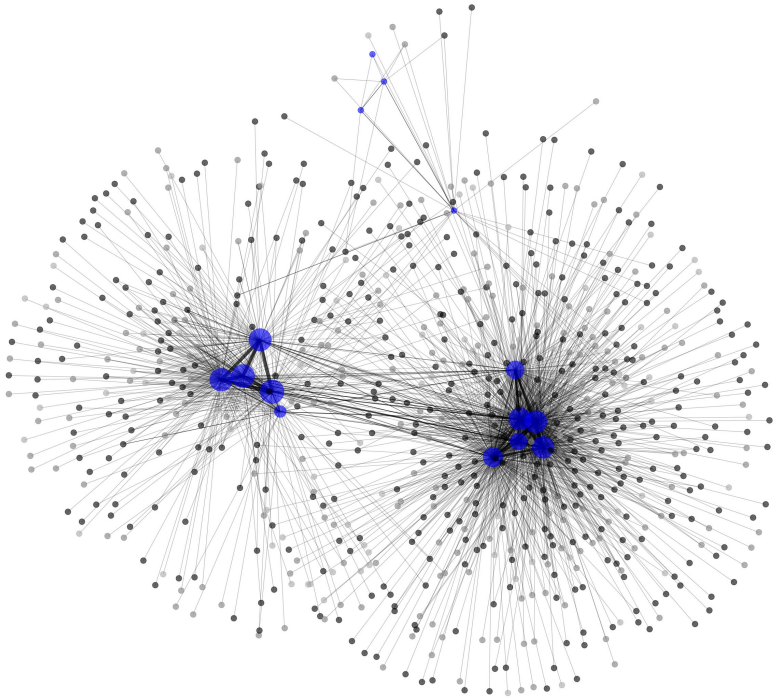
- COVID-19 pushed many employees home in an abrupt manner
  - Companies varied in their preparedness
- Rapid response by organizations to continue business operations
  - Corporate infrastructure hastily set up and exposed to permit continued access
  - Normally unsupported devices now allowed to access corporate information
- Balancing act between business operations and existing security practices
- Attacks using coronavirus and COVID-19 as a launching platform
- The confusion of new policies lend itself an open door for phishing attacks

Corporate Office vs. Home Office

- Professionally managed vs. individually managed
- Device ecosystem very different than corporate environments
  - IoT devices not normally found on organizational networks
  - Consumer-grade hardware and systems lend themselves more common to misconfigurations and stale updates
- Very different set of threats in the home environment
- Actors are becoming more patient to increase their chance of success[0][1]
- Corporate devices are now persistently available in home office environments

[0] https://news.sophos.com/en-us/2020/05/27/netwalker-ransomware-tools-give-insight-into-threat-actor/
[1] https://www.nytimes.com/2020/06/25/us/politics/russia-ransomware-coronavirus-work-home.html

Comparing Security of Residential vs. Corporate Networks



Example of company with two office locations. Blue dots represent corporate IPs; black dots represent connected residential IPs.

- We wanted to understand the general security state of home networks and how they compared to the corporate network. Specifically, we wanted to see what was unique between each environment.
- To do that, we had to understand the corporate network, as well as at least a sample of corporate-associated residential networks, and then compare between the two.
- Significant noise reduction to remove carrier-grade NATs, cellular networks, shared IP space, etc.

The Unprecedented Shift to Remote Work

During the period of March 2020, we looked at a sample size of **41,000 organizations** to understand the difference between corporate networks and Work From Home-Remote Office (WFH-RO) networks from a cyber-risk perspective.

84%

of
Education sector traffic
shifted off network.

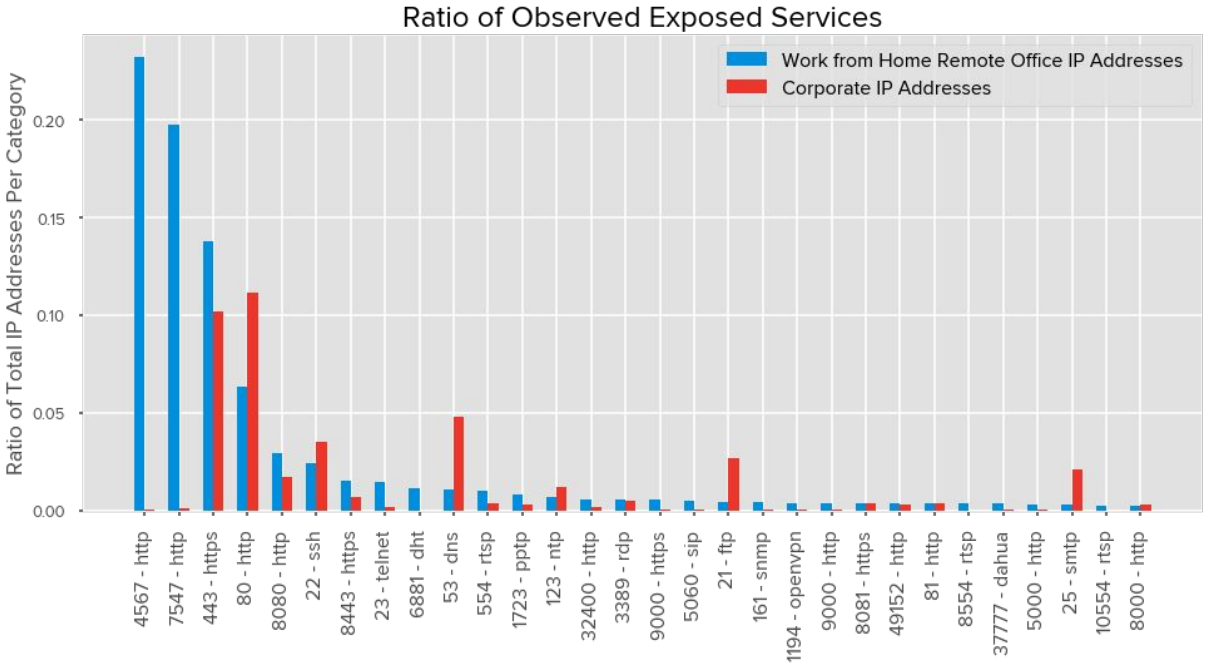
63%

of
Government/Politics
sector traffic
shifted off network.

35%

of
Finance sector traffic
shifted off network.

Network Perimeter

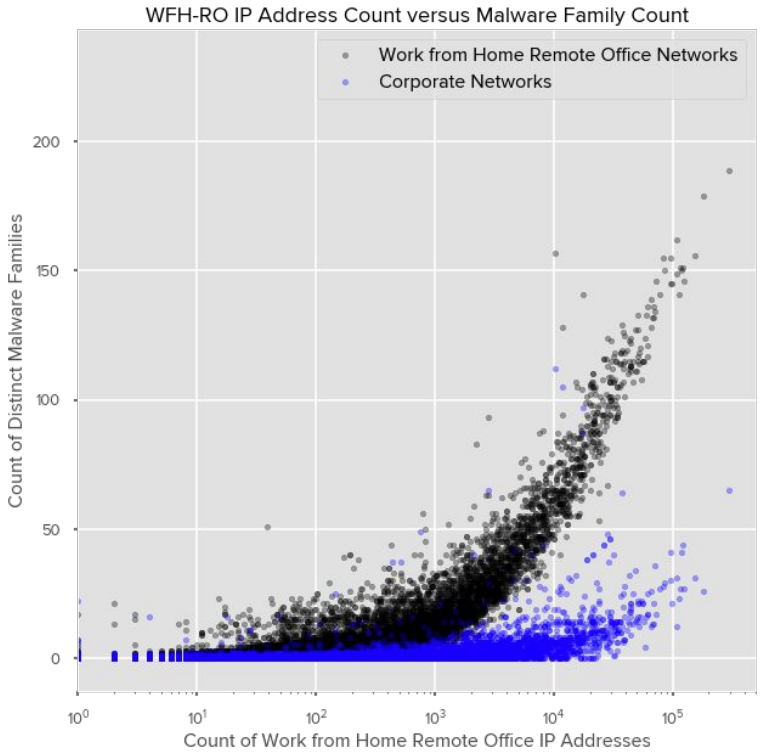


- The attack surface is quite different between the home and corporate environment.
- **15%** of home offices have exposed modem control interfaces, while **22%** that have a service exposed include an administrative interfaces for their routers.

Figures from the **BitSight "Identifying Unique Risks of Work from Home - Remote Office Networks" White Paper**
https://info.bitsight.com/identifying-unique-risks-of-work-from-home-remote-office-networks

Malware

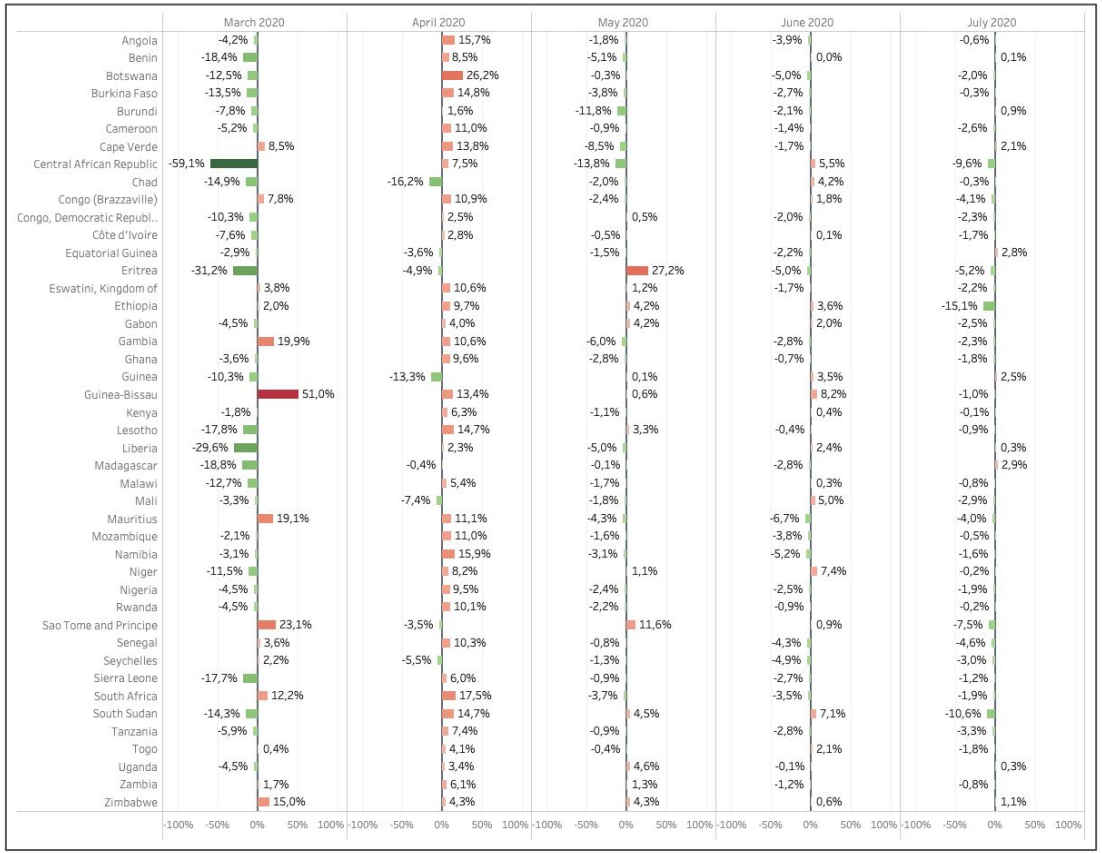
- Home networks are **3.5 times** more likely to have at least one malware family than corporate networks, and **7.5 times** more likely to have at least five different malware families.
- As the size of the organization increases, so does the complexity of managing infrastructure, processes, and human practices within the physical and digital boundary of the corporate network.
- About **13%** of companies were observed to have malware during this period, and **45%** of residential networks.



Figures from the **BitSight "Identifying Unique Risks of Work from Home - Remote Office Networks" White Paper**
https://info.bitsight.com/identifying-unique-risks-of-work-from-home-remote-office-networks

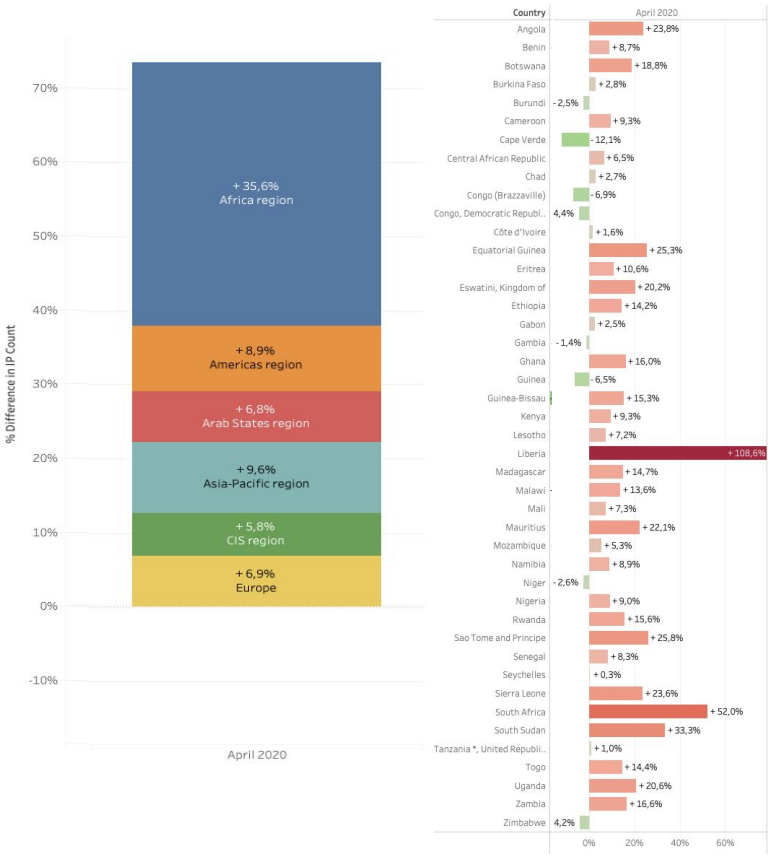
Africa - Torrent Activity Monthly Change

(% Growth Rate to Previous Month)



Remote Access Applications and Protocols

(% Delta between January 1st and April 30th)



Thank you

francisco.fonseca@bitsight.com
www.bitsight.com