BITSIGHT

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



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.



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.



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** <u>https://info.bitsight.com/identifying-unique-risks-of-work-from-home-remote-office-networks</u>

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** <u>https://info.bitsight.com/identifying-unique-risks-of-work-from-home-remote-office-networks</u>

Africa - Torrent Activity Monthly Change

(% Growth Rate to Previous Month)

	1 001			40.001	1.001		2.001		0.001	1
Angola	-4,2%			15,7%	-1,8%		-3,9%		-0,6%	
Benin	-18,4%			8,5%	-5,1%			0,0%		0,1%
Botswana	-12,5% 🔳			26,2%	-0,3%		-5,0%		-2,0%	
Burkina Faso	-13,5% 🔳			14,8%	-3,8%		-2,7%		-0,3%	
Burundi	-7,8% 📕			1,6%	-11,8% 🔳		-2,1%			0,9%
Cameroon	-5,2%			11,0%	-0,9%		-1,4%		-2,6%	1. I.
Cape Verde		8,5%		13,8%	-8,5%		-1,7%			2,1%
Central African Republic	-59,1%			7,5%	-13,8%			5,5%	-9,6%	
Chad	-14,9%		-16,2%		-2,0%			4,2%	-0,3%	
Congo (Brazzaville)		7,8%		10,9%	-2,4%			1,8%	-4,1%	
ngo, Democratic Republ.	-10,3%			2,5%		0,5%	-2,0%		-2,3%	
Côte d'Ivoire	-7.6%			2.8%	-0.5%	100000		0.1%	-1.7%	
Fouatorial Guinea	-2.9%		-3.6%		-1.596		-2.2%			2.8%
Eritrea	-31.2%		-4.9%			27.2%	-5.0%		-5,2%	1.000
Eswatini, Kingdom of		3.8%	.,570	10.6%		1.2%	-1.7%		-2 296	
Ethionia		2 0%		9 7%		4 2%	2,770	3.6%	-15 1%	
Gaboo	-4 596	2,070		4.0%		A 296		2.0%	-2 5%	
Gapon	***,370	10.0%		10.6%	E 004	17,270	3.00/	2,070	2,370	
Chana	2 604	19,970		0.6%	-0,078		-2,076		-2,370	
Griana	-3,070		12.20	9,070	-2,070	0.10/	-0,770	2.50/	-1,070	2.50
Guinea	-10,3%	E1.00	-13,3%	17.40		0,1%		3,5%	1.000	2,5%
Guinea-Bissau		51,0%		13,4%		0,6%		8,2%	-1,0%	
Kenya	-1,8%			6,3%	-1,1%			0,4%	-0,1%	
Lesotho	-17,8%			14,7%		3,3%	-0,4%		-0,9%	1
Liberia	-29,6%			2,3%	-5,0%			2,4%		0,3%
Madagascar	-18,8%		-0,4%		-0,1%		-2,8%			2,9%
Malawi	-12,7% 🔳			5,4%	-1,7%			0,3%	-0,8%	
Mali	-3,3%		-7,4%		-1,8%			5,0%	-2,9%	
Mauritius		19,1%		11,1%	-4,3%		-6,7%		-4,0%	
Mozambique	-2,1%			11,0%	-1,6%		-3,8%		-0,5%	
Namibia	-3,1%			15,9%	-3,1%		-5,2%		-1,6%	
Niger	-11,5%			8,2%		1,1%		7,4%	-0,2%	
Nigeria	-4,5%			9,5%	-2,4%		-2,5%		-1,9%	
Rwanda	-4,5%			10,1%	-2,2%		-0,9%		-0,2%	
Sao Tome and Principe	82.4	23,1%	-3,5%			11,6%		0,9%	-7,5%	
Senegal		3,6%		10,3%	-0,8%		-4,3%		-4,6%	
Sevchelles		2,2%	-5,5%		-1,3%		-4,9%		-3.0%	
Sierra Leone	-17,7%	Concerned I		6.0%	-0,9%		-2.7%		-1 2%	
South Africa		12.2%		17.5%	-3.7%		-3.5%		-1.9%	
South Sudan	-14 3%			14 7%	-// /-	4 5%	5,5.0	7 196	-10.6%	
Tanzania	-5 9%			7 4%	-0 996	.,	-2 8%	.,1.0	-3 396	
Togo	5,570	0.4%		4 196	-0.4%		2,070	2 196	-1.8%	
llaseda	A 504	0,770		3 496	-0,470	4 696	-0.194	2,170	-1,070	0.3%
uganda Zambia	-4,370	1 704		6 104		1 294	-0,1%		0.00/	0,370
Zampia		1, / 70		0,1%		1,370	-1,2%	0.000	-0,8%	1.10/



Remote Access Applications and Protocols (% Delta between January 1st and April 30th)







Thank you

<u>francisco.fonseca@bitsight.com</u> www.bitsight.com