

Your Biggest Security Adversaries Might Be Wearing Pajamas!

SEC1885

James Brodsky

Sr Director Security Strategists | Splunk



Forward-Looking Statements



During the course of this presentation, we may make forward-looking statements regarding future events or plans of the company. We caution you that such statements reflect our current expectations and estimates based on factors currently known to us and that actual events or results may differ materially. The forward-looking statements made in the this presentation are being made as of the time and date of its live presentation. If reviewed after its live presentation, it may not contain current or accurate information. We do not assume any obligation to update any forward-looking statements made herein.

In addition, any information about our roadmap outlines our general product direction and is subject to change at any time without notice. It is for informational purposes only, and shall not be incorporated into any contract or other commitment. Splunk undertakes no obligation either to develop the features or functionalities described or to include any such feature or functionality in a future release.

Splunk, Splunk>, Data-to-Everything, D2E and Turn Data Into Doing are trademarks and registered trademarks of Splunk Inc. in the United States and other countries. All other brand names, product names or trademarks belong to their respective owners. © 2020 Splunk Inc. All rights reserved



- Sr. Director, Global Security Strategists
- Lead a team of Splunk security strategists across the US, UK, Australia
- Have been involved with security@Splunk since my start in 2013
- .conf Splunking the Endpoint! for FIVE years
- BOTS 2016-2020. BOTN 2017-2018.
- Windows Event Code Analysis App, CSC 20 Whitepaper, FFIEC Whitepaper (co-author), other compliance, Tripwire apps, blogs, Sysmon contributions, etc, etc....



The End of an Era?



.conf2015

Splunking the Endpoint

James Brodsky
Staff Engineer/Security SME, Splunk
brodsky@splunk.com

splunk>



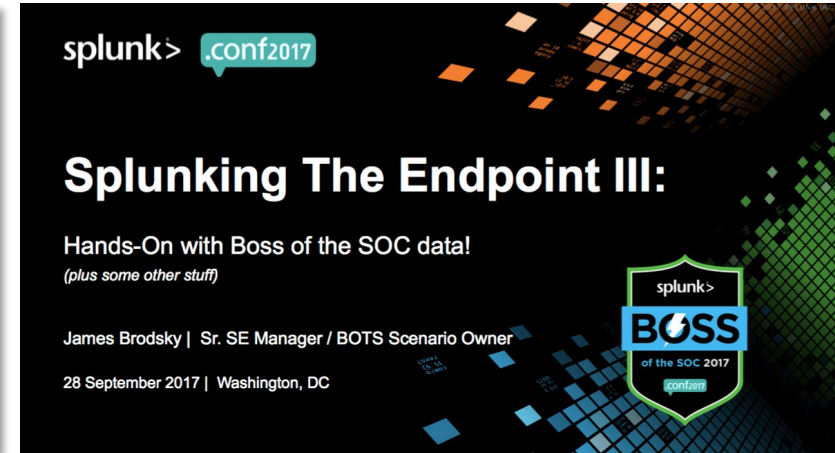
**Splunking the Endpoint: "Hands on!"
Ransomware Edition**

James Brodsky
Guy with beard | Splunk

Dimitri McKay
Guy with larger beard | Splunk

.conf2016

splunk>




splunk> **.conf2017**

Splunking The Endpoint III:

Hands-On with Boss of the SOC data!
(plus some other stuff)

James Brodsky | Sr. SE Manager / BOTS Scenario Owner
28 September 2017 | Washington, DC



.conf18

splunk>



Splunking The Endpoint IV

A New Hope

SEC1378

brodsky@splunk.com | sr. security specialist manager | manager of security kittens

October 2018 | Version 1.0



.conf19

splunk>



**SPLUNKING THE ENDPOINT V:
Enough Already! (SEC2007)**

brodsky@splunk.com
Director Global Security Strategists | Security Kittens

October, 2019
V1.0

splunk> **.conf19**

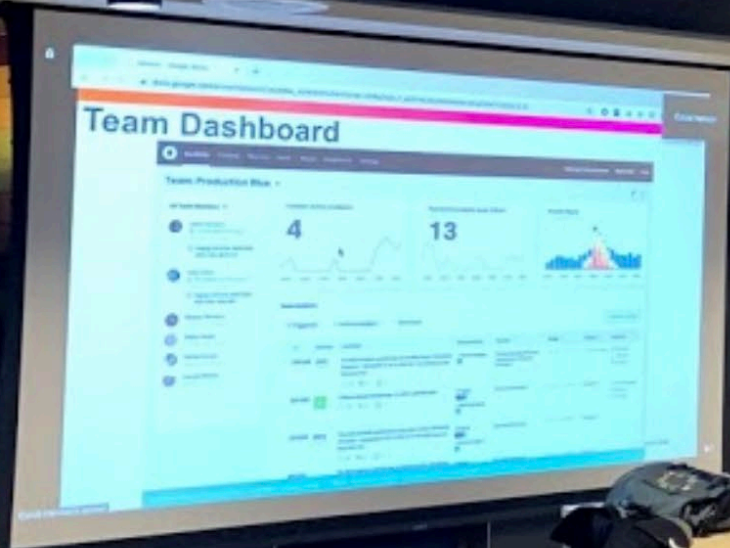
**Never fear – all of
this history is
relevant!**

Our beautiful new Splunk Boulder office in October, 2019!

splunk>



Fancy open spaces, happy Splunkers, excellent snacks...





That exact same space, late March, 2020.



Our new reality.

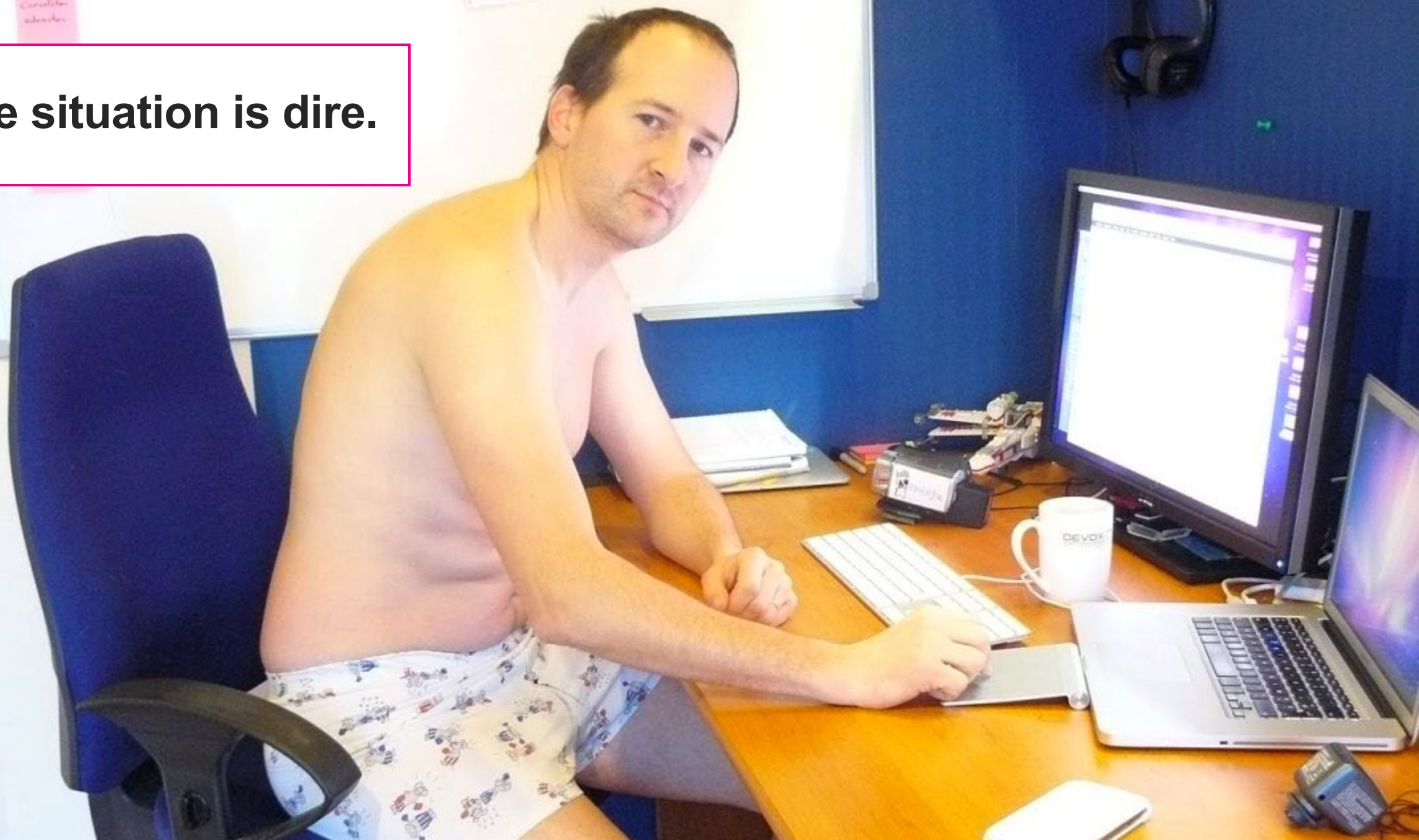
A dimly lit, abandoned office with a checkered floor, desks, and a cabinet with a 'broken' sign. The room is empty, with a few desks and chairs scattered around. A cabinet in the foreground has a yellow sign that says 'broken'. The lighting is low, with a few overhead lights visible.

In the next **27** minutes...

- Just how much has the work world changed?
- What are the biggest WFH security concerns?
- What have we seen, how can Splunk help?
- What to do next?

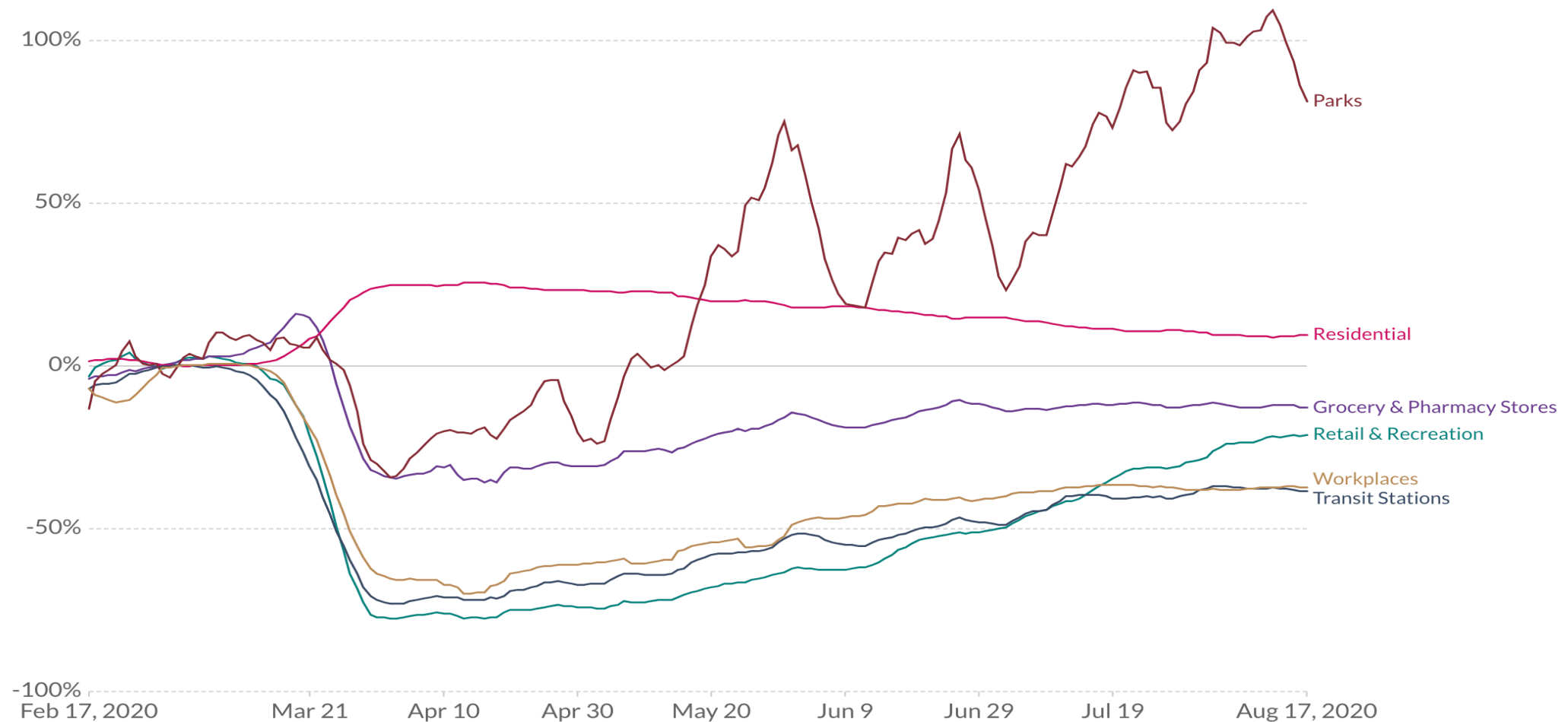
(And throughout – the remote work BOTS scenario!)

The situation is dire.



How did the number of visitors change since the beginning of the pandemic?, United Kingdom

The data shows how visitors to (or time spent in) categorized places change compared to baseline days – the median value from the 5-week period from January 3rd to February 6th 2020. This index is smoothed to the rolling 7-day average.



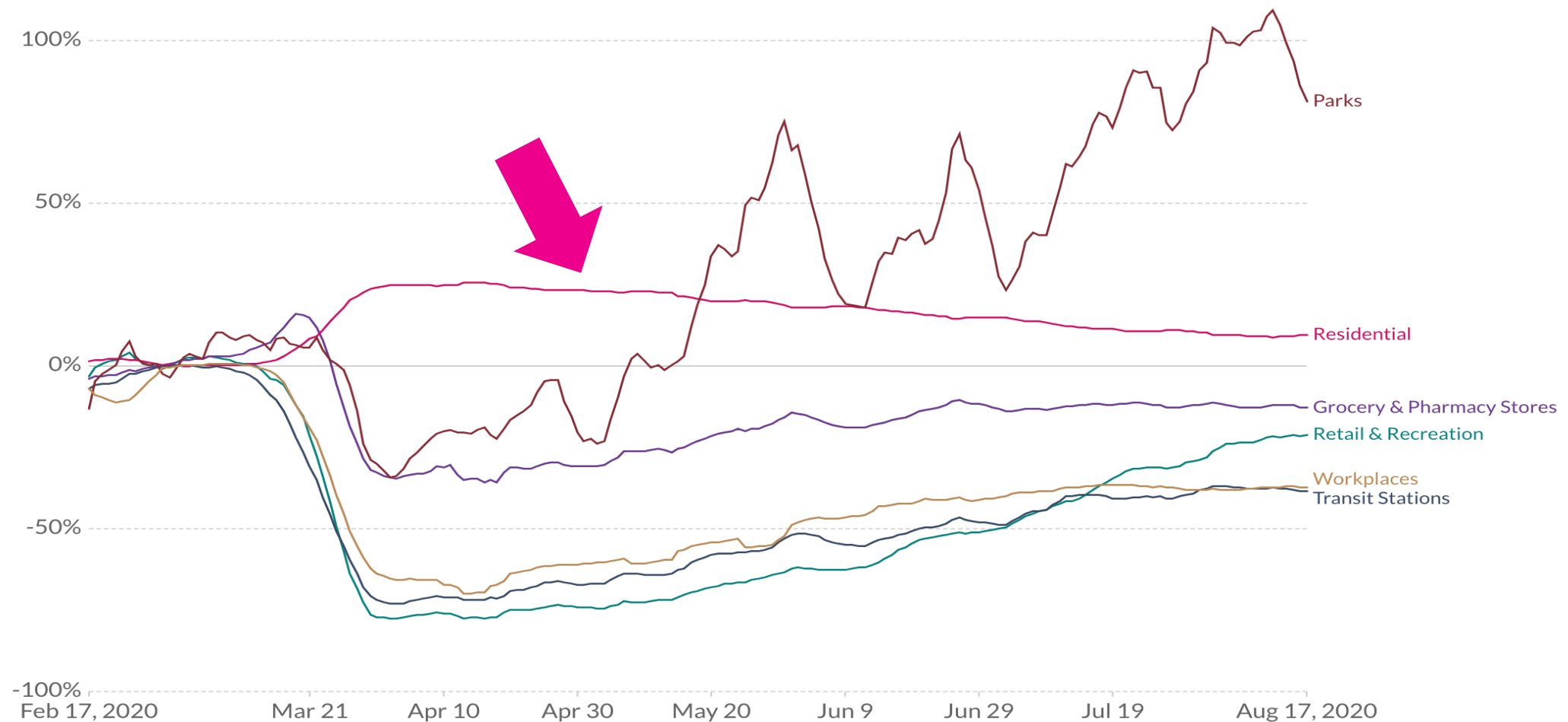
Source: Google COVID-19 Community Mobility Trends – Last updated 21 August, 20:31 (London time)
Note: It's not recommended to compare levels across countries; local differences in categories could be misleading.

OurWorldInData.org/coronavirus • CC BY



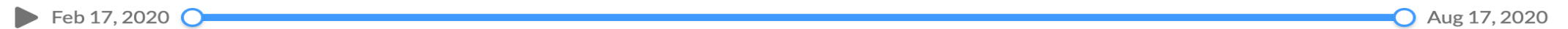
How did the number of visitors change since the beginning of the pandemic?, United Kingdom

The data shows how visitors to (or time spent in) categorized places change compared to baseline days – the median value from the 5-week period from January 3rd to February 6th 2020. This index is smoothed to the rolling 7-day average.



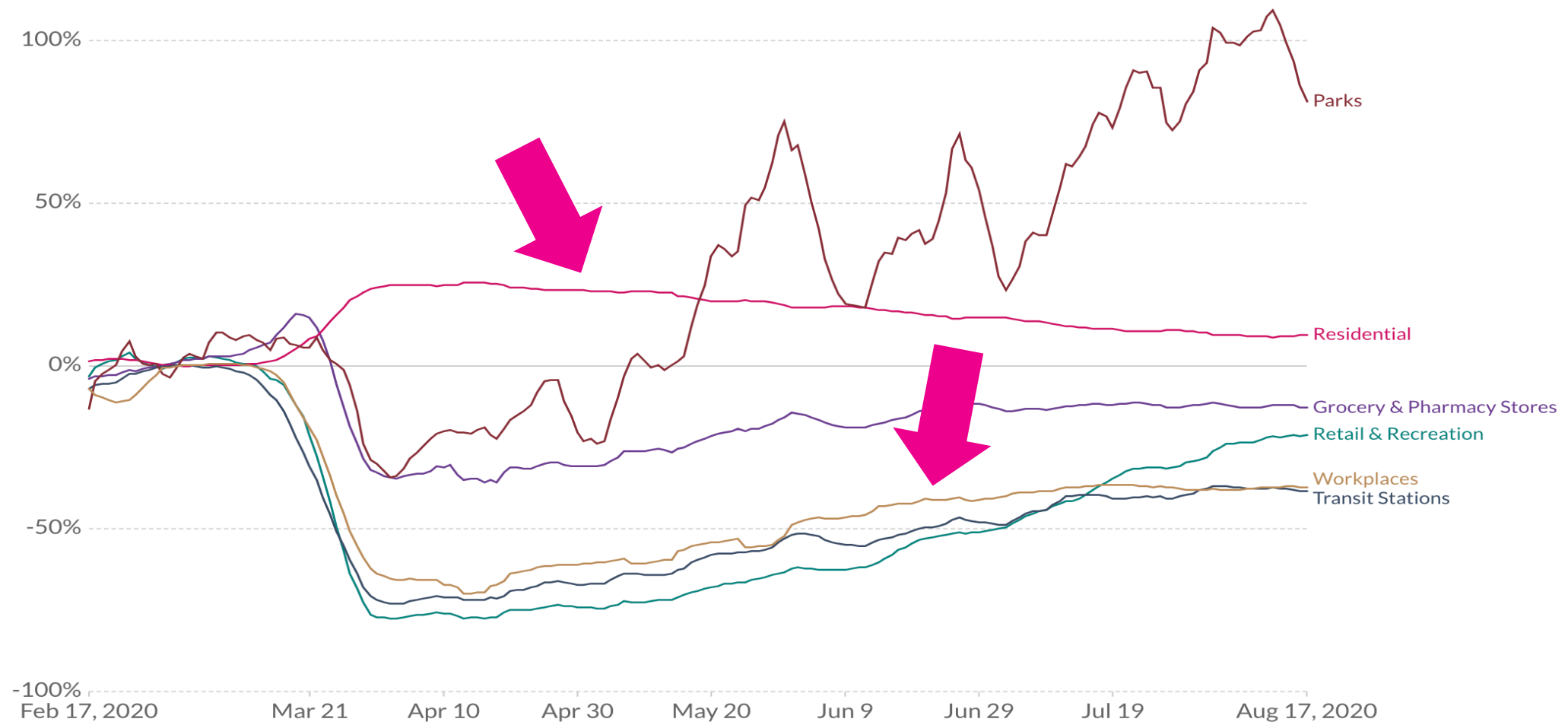
Source: Google COVID-19 Community Mobility Trends – Last updated 21 August, 20:31 (London time)
Note: It's not recommended to compare levels across countries; local differences in categories could be misleading.

OurWorldInData.org/coronavirus • CC BY



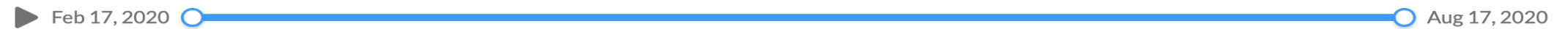
How did the number of visitors change since the beginning of the pandemic?, United Kingdom

The data shows how visitors to (or time spent in) categorized places change compared to baseline days – the median value from the 5-week period from January 3rd to February 6th 2020. This index is smoothed to the rolling 7-day average.



Source: Google COVID-19 Community Mobility Trends – Last updated 21 August, 20:31 (London time)
Note: It's not recommended to compare levels across countries; local differences in categories could be misleading.

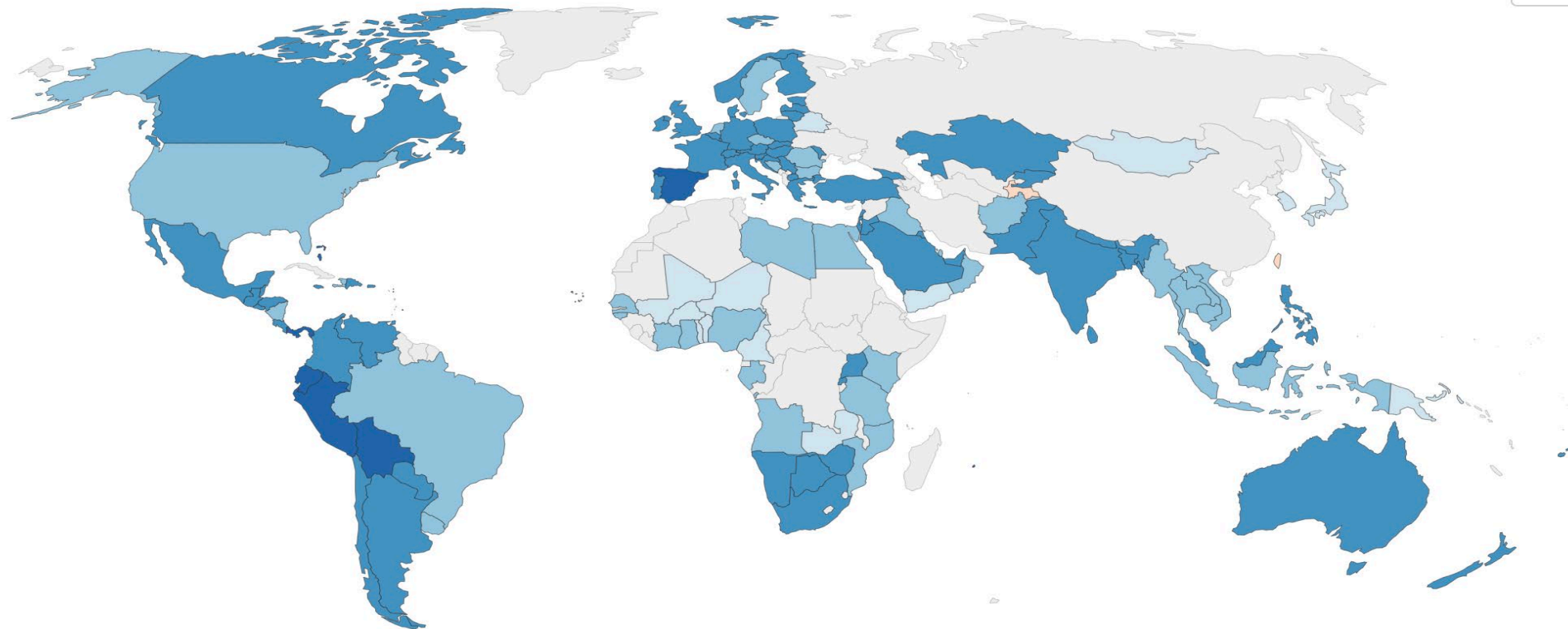
OurWorldInData.org/coronavirus • CC BY



Workplaces: How did the number of visitors change since the beginning of the pandemic?, Apr 13, 2020

Change in visitor numbers is measured relative to a baseline day; a baseline day is the median value from the 5-week period between Jan 3rd and Feb 6th 2020. This index is smoothed to the rolling 7-day average.

World

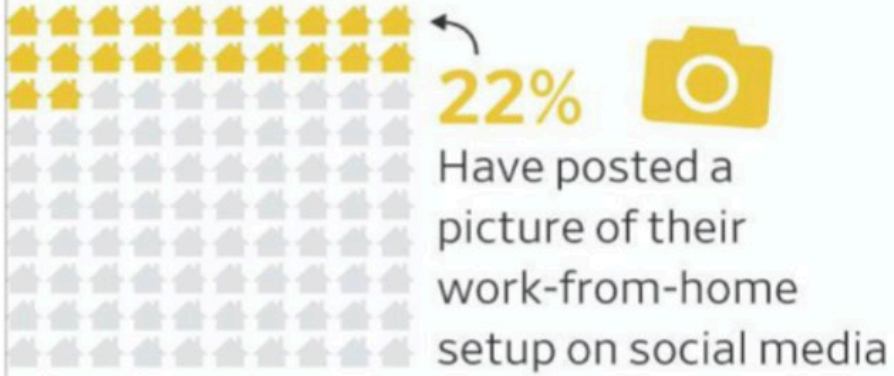


Source: Google COVID-19 Community Mobility Trends, last updated 21 August, 20:31 (London time)
Note: It's not recommended to compare levels across countries as there are significant differences in categories that could be misleading.

OurWorldInData.org/coronavirus • CC BY

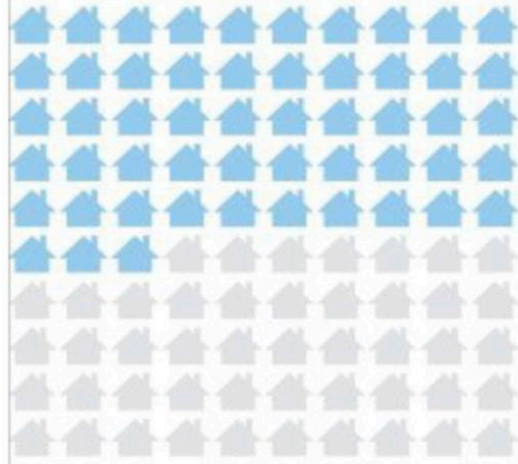
Feb 17, 2020  Aug 17, 2020

People who work with personally identifiable information and are newly working from home due to the pandemic



Add WSJ/IBM Attribution

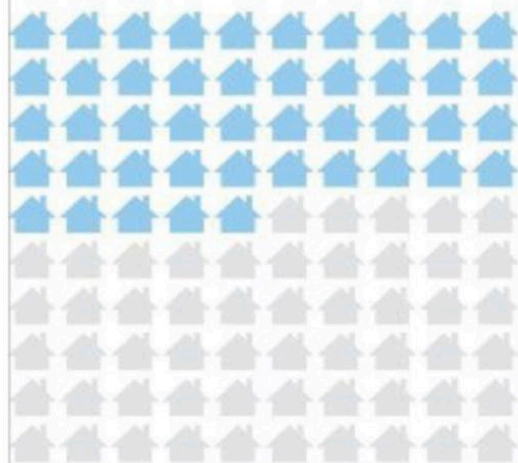
People who are newly working from home due to the pandemic



53%



Use a personal laptop or computer for work



45%



Say employer hasn't provided security training during work from home

“98% of 200 survey respondents moved at least 21% of workforce to remote work.”

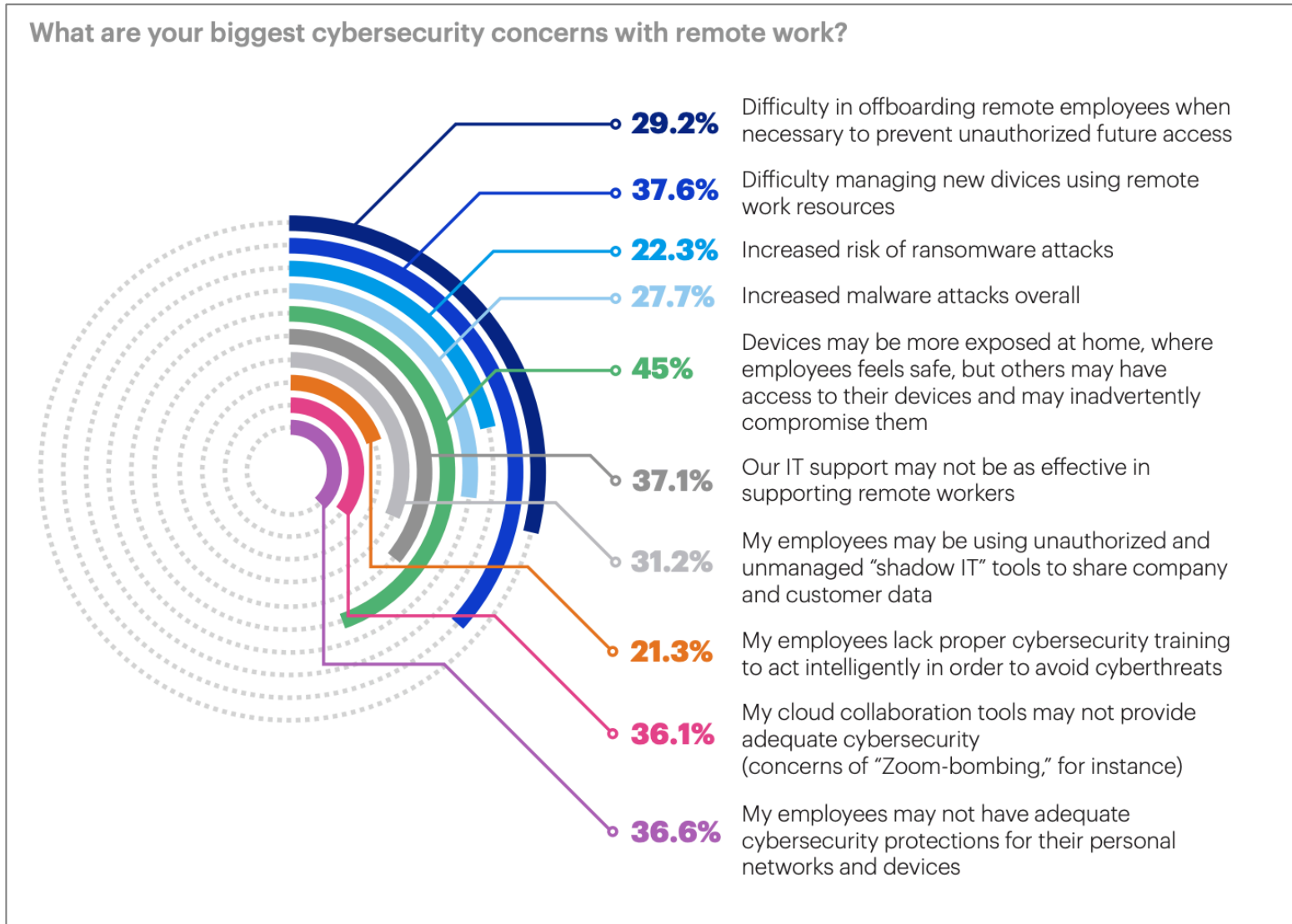
— Malwarebytes, 8/20



**Any concerns with security issues
when employees WFH?**



Yep.



Add Malwarebytes attribution

And, yep.



Said they paid unexpected expenses specifically to address a cybersecurity breach or malware attack following shelter-in-place orders.



Said they faced a security breach as a result of a remote worker.



Admitted that, for their employees, cybersecurity was not a priority, while 5 percent admitted their employees were a security risk and oblivious to security best practices.



Admitted they're using personal devices for work-related activities more than their work-issued devices, which could create new opportunities for cyberattacks.

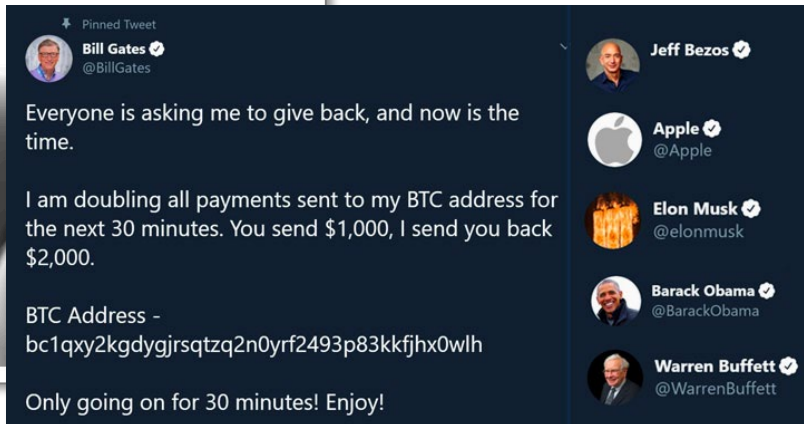
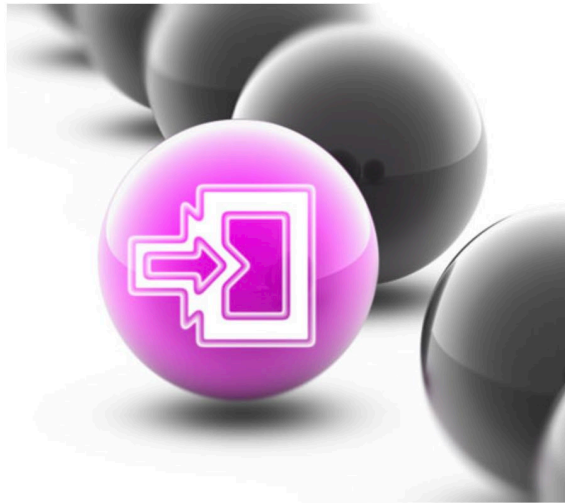
Anything bad happen?

Hacker Leaks 900 Enterprise Server Passwords on Dark Web

Threat intelligence firm KELA shared a list of more than 900 Secure VPN enterprise server usernames and passwords on the Dark Web, which a hacker had posted on the dark web.



Not Enough Organizations Using BYOD Anti-Malware Software Protection



JOINT CYBERSECURITY ADVISORY

TLP:AMBER

Product ID: A20-233A August 20, 2020

Cyber Criminals Take Advantage of Increased Telework Through Vishing Campaign

SUMMARY

The Federal Bureau of Investigation (FBI) and Cybersecurity and Infrastructure Security Agency (CISA) are issuing this advisory in response to a voice phishing (vishing) campaign.

The COVID-19 pandemic has resulted in a mass shift to working from home, resulting in increased use of corporate virtual private networks (VPNs) and elimination of in-person verification. In mid-July 2020, cybercriminals started a vishing campaign—gaining access to employee tools at multiple companies with indiscriminate targeting—with the end goal of monetizing the access. Using vished credentials, cybercriminals mined the victim company databases for their customers' personal information to leverage in other attacks. The monetizing method varied depending on the company but was highly aggressive with a tight timeline between the initial breach and the disruptive cash-out scheme.

How hackers are using COVID-19 to find new phishing victims





Email

VPN

Proxy

Badge

Endpoint

Auth

DNS

Ticketing

Staff is home, with their cats. What should we collect from them and why?

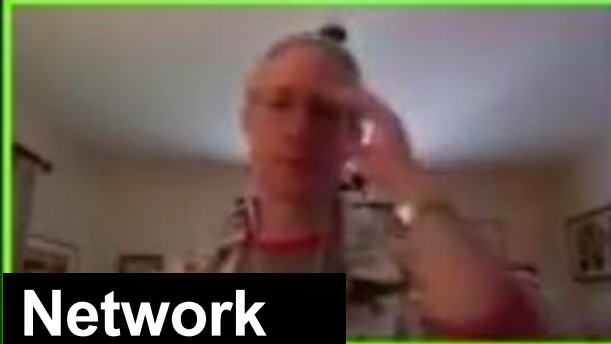
The 12 Wonderful WFH Datasources



VPN



Endpoint



Network



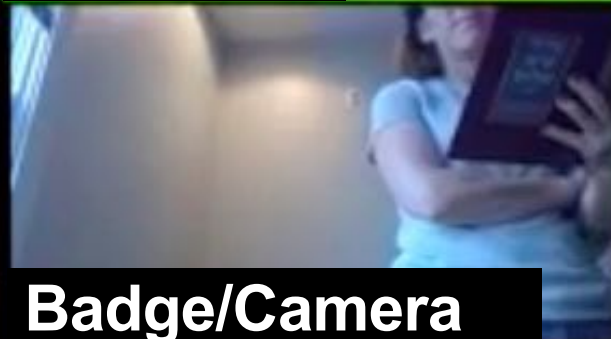
Email



Authentication



DNS



Badge/Camera



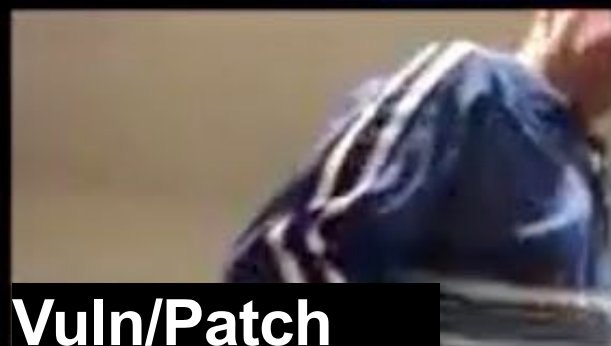
Web Conf



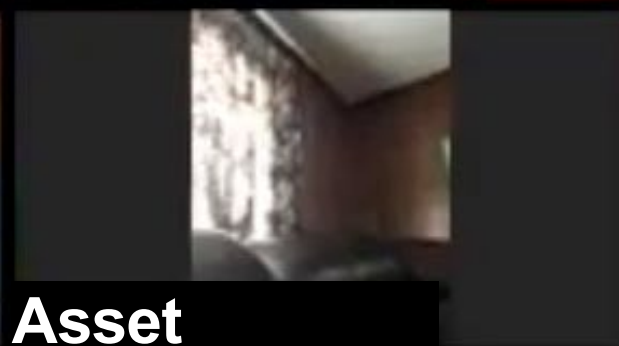
Ticketing



WiFi History



Vuln/Patch



Asset



What can we do
in Splunk with
VPN data?

How VPN works



Internet

Your house

Corporate
Resources

1. VPN Examples: Cisco Anyconnect and CESA/NVM, PAN GlobalProtect, Fortinet, Zscaler, Juniper Pulse

- Is your VPN working properly? (business continuity)
- Usage patterns (usual and unusual)
- Authentication issues (odd country, odd behavior per user/role)
- Licensing issues
- Vulnerabilities on the client and the concentrators
- Config issues (split tunnel vs 100% of traffic, proper encryption method...)
- BYOD device being used for VPN
- Special capabilities in Cisco (CESA/NVM) and with GlobalProtect's config check and Pulse Secure Host Checker

DATA SOURCES: VPN auth logs, operational logs, vuln scanner logs

DATA MODELS: Network Traffic, Authentication, Network Sessions,

APPS: Core, InfoSec App, ES, UBA, Security Essentials



BOTS Example – Pulse Secure VPN



Palo Alto Host Information

```
Aug 3 15:34:53 <pan device> 1,2018/08/03
15:34:53,010401003236,HIPMATCH,0,16,2018/08/03 15:34:53,<user>,vsys1,<user
endpoint>,Mac,<internal ip>,Has Disk
Encryption,1,object,0,0,25256,0x0,11,42,0,0,,<pan device>
```

```
[pan:hipmatch]
SHOULD_LINEMERGE = false
REPORT-search = extract_hipmatch
FIELDALIAS-virtual_system = vsys as virtual_system
# Field Aliases to map sepcific fields to the Splunk Common
Information Model--Intrusion Detection
```

```
FIELDALIAS-src_for_pan_hipmatch = src_ip as src
FIELDALIAS-dvc_for_pan_hipmatch = host as dvc
FIELDALIAS-user_for_pan_hipmatch = src_user as user
LOOKUP-vendor_info_for_pan_hipmatch = pan_vendor_info_lookup
sourcetype OUTPUT vendor,product,vendor_product
```

<https://www.paloaltonetworks.com/documentation/71/pan-os/web-interface-help/globalprotect/objects-globalprotect-hip-objects>

<https://www.paloaltonetworks.com/documentation/80/globalprotect/globalprotect-admin-guide/host-information/configure-hip-based-policy-enforcement.html>

hip_name

7 Values, 100% of events Selected Yes No

Reports

Top values Top values by time Rare values

Events with this field

Values	Count	%
MAC Disk Encryption	52	35.616%
MAC Casper	25	17.123%
Has Disk Encryption	22	15.068%
MAC Antivirus	20	13.699%
Windows Disk Encryption	15	10.274%
Compliance	6	4.11%
Windows Antivirus	6	4.11%

HIP Object (Read Only)

General

Mobile Device

Patch Management

Firewall

Antivirus

Anti-Spyware

Disk Backup

Disk Encryption

Data Loss Prevention

Custom Checks

Antivirus

Is Installed Real Time Protection yes

Virus Definition Version Within

Days 45

Product Version None

Last Scan Time Not Available

1 Item

Vendor	Product
<input type="checkbox"/> Symantec Corp.	Symantec Endpoint Protection

Exclude Vendor

OK Cancel

Cisco AnyConnect Network Visibility Module (NVM)



Application – User – Device – Location – Destination

IPFIX-Based Record (Source IP, Destination IP, etc)

Unique Device ID (correlate records from same endpoint device)

Device Name (bsmith-WIN) and OS Version (Window 7)

Domain\User Name (AMER\bsmith)

Local DNS (starbucks.com), Target DNS (-> amceco.box.com)

Interface (Intel (R) Dual Band Wireless)

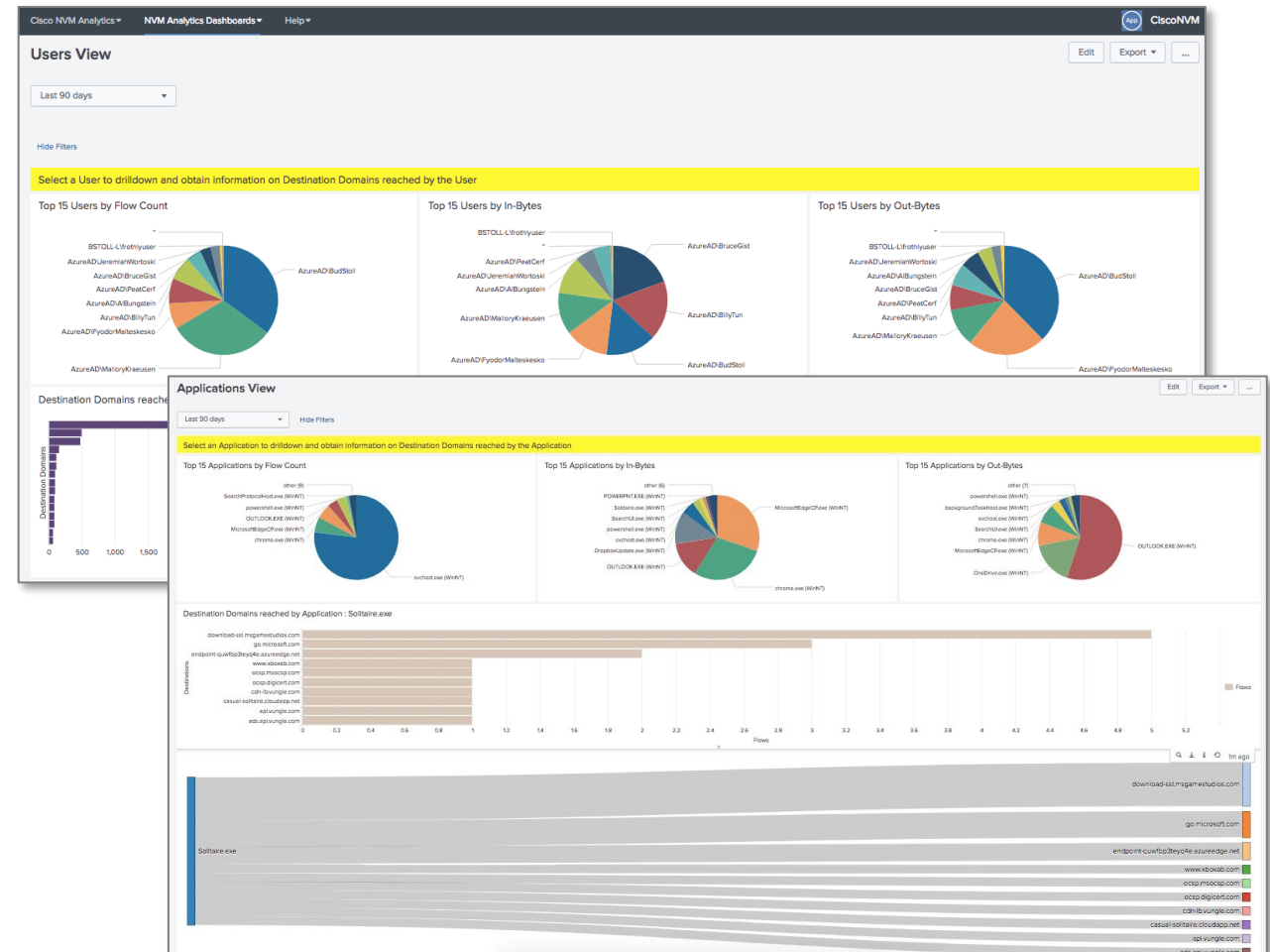
Process/Container Name (iexplorer.exe), Process ID (hash)

Parent Process Name (foobar.exe) Parent ID (hash)

Cisco NVM Details

- Windows, macOS, Android/Knox
- Does not need to be connected to VPN to collect
- Processes mapped to network activity (but must generate network activity)
- Needs an Apex license (but you can try it out no problem...)
- Cisco-supported Splunk App contains a basic IPFIX collector, or use your own
- Data comes into Splunk from collector via Syslog
- Tested at scale!

<https://www.cisco.com/c/en/us/support/docs/security/anyc-connect-secure-mobility-client/200600-Install-and-Configure-Cisco-Network-Visi.html>





How
about
Endpoint
data?

2. Endpoint Examples: Crowdstrike, Carbon Black, Tanium, Sysmon, Windows Events, Osquery, Cisco CESA/NVM

- Applications in use
- Communications down to the process/app
- Hardware/Software Inventory
- Malicious hashes
- File/Network activity for DLP
- DNS query data
- Worker Productivity monitoring
- Critical for MITRE ATT&CK mapping

DATA SOURCES: Windows Event logs, Endpoint Alerts, granular endpoint data

DATA MODELS: Endpoint, Authentication, Network Sessions, DLP, Change Analysis

APPS: Core, SSE, InfoSec App, ES, UBA, Phantom



BOTS Example – OSQUERY FIM



**Network
data is
also key**

3. Network Traffic Examples:

Cisco/Palo/Fortinet/Checkpoint firewalls, Bluecoat/Palo for proxy, AWS VPC Flow logs

- What's talking to what, how much, for how long, and when
- Track bandwidth utilization
- Known malicious communications by IP/country
- Application volumes (e.g. Zoom traffic)
- Productivity monitoring via proxy categories

DATA SOURCES: Firewall/Proxy logs

DATA MODELS: Network Traffic, Web

APPS: Core, SSE, InfoSec App, ES, UBA, Phantom

.conf20

splunk>



BOTS Example – Stream



**Don't
forget
Email**

4. Email Data Examples: Proofpoint, STOQ, Microsoft message trace, Cisco ESA, gmail TA

- Subject lines/body/attachment - anything with COVID-19 or coronavirus in the content?
- Phishing analysis with Phantom processing self-reported messages
- Detonate malicious attachments via Sandbox
- Remove malicious email before users can open

DATA SOURCES: Email processing/appliance logs

DATA MODELS: Email

APPS: Core, SSE, InfoSec App, UBA, Phantom



SECURITY

How Do I Add COVID (or Any) Threat Intelligence From the Internet to Splunk Enterprise Security?

Dear Buttercup...

By [Ryan Kovar](#) April 08, 2020

Dear Buttercup,

My dog catching company has been targeted multiple times by ransomware using COVID domains. We have [Splunk Enterprise Security](#) installed, but we can't afford any of those fancy Threat Intelligence data feeds. I just want to get threat intelligence data into ES without having to have a vendor feed. Can you help me add threat intelligence data to find and detect domains, URLs, and hashes about COVID, without paying any money?

*Sincerely,
Old Man Kensey from Athens, Georgia*



I'm happy to help you out, Mr. Kensey! Many organizations struggle with buying or affording threat intelligence to plug into Enterprise Security. In fact, the dapperly handsome [Ryan Kovar](#) wrote about how to [pick the best threat intelligence for your company](#) back in 2016. But if you are facing a budget crisis and/or don't have time to develop your own threat intelligence data for COVID, we can help you out. The recent crisis has brought the best (and the worst as evidenced by your issues) out of people. Several [self-organized groups](#) have stood up MISP servers that are full of vetted and reviewed intelligence that you can gain access to¹. The most prominent



BOTS Example – Gmail Audit TA



Authentication:
who is coming
in the front
door?



5. Authentication data examples: Azure AD, conventional AD, Okta/Duo/other SSO, 2FA/MFA

- Is 2FA/MFA configured and working on all services?
- Without MFA, passwords are easy to guess
- Unusual access patterns
- Unusual credential resets
- Password spray attempts
- Evidence of reconnaissance efforts/credential stuffing attacks

DATA SOURCES: Authentication logs from all services

DATA MODELS: Authentication

APPS: Core, SSE, ES, InfoSec App, UBA, Phantom

Krebs on Security

In-depth security news and investigation



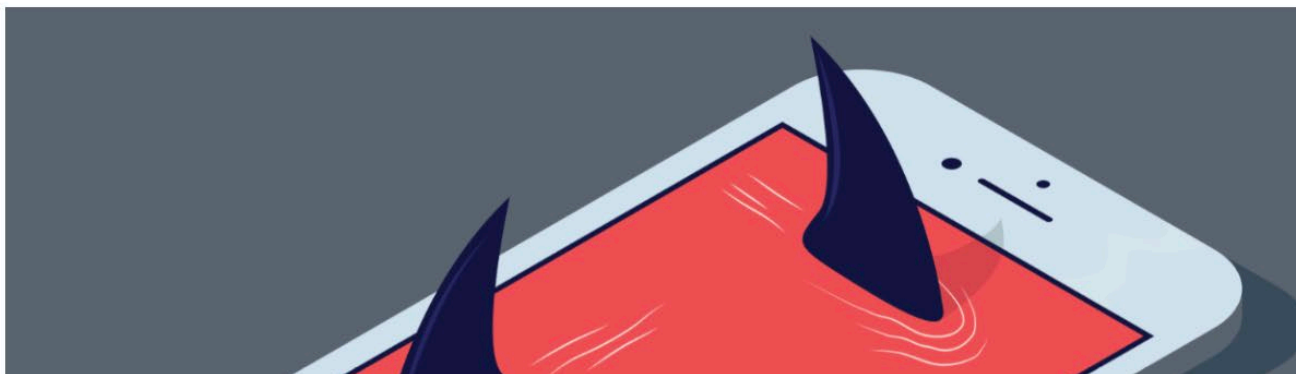
ADVERTISING/SPEAKING

ABOUT THE AUTHOR

19 Voice Phishers Targeting Corporate VPNs

AUG 20

The COVID-19 epidemic has brought a wave of email phishing attacks that try to trick work-at-home employees into giving away credentials needed to remotely access their employers' networks. But one increasingly brazen group of crooks is taking your standard phishing attack to the next level, marketing a voice phishing service that uses a combination of one-on-one phone calls and custom phishing sites to steal VPN credentials from employees.



Advertisement

What is your ~~mother's maiden name?~~ security solution doing for you?

oktaOkta.com/TheAnswer

.conf20

splunk>



BOTS Example – Unusual RDP/VNC or Superman

DNS

tells you what
those remote
workers are
looking for...

The screenshot shows a web browser window with a Google search for "cat videos". The search results page displays a video player for "The funniest and most humorous cat videos ever! - Funny cat ..." by Tiger Productions, with a duration of 10:16. Below the video player, there are two search results for YouTube videos:

- [TOP 10 BEST CAT VIDEOS OF ALL TIME! - YouTube](#)
We've scoured the internet and found the cutest and funniest **cat videos** of all time. Any we missed? Let us ...
2:40
Sep 6, 2012 - Uploaded by WatchTheDaily
- [THE BEST CUTE AND FUNNY CAT VIDEOS OF 2019 ...](#)
THE BEST CUTE AND FUNNY **CAT VIDEOS** OF 2019!. 4,487,084 views. 4.4M views. • Dec 30, 2019.
58:58
Dec 30, 2019 - Uploaded by Rufus

6. DNS Data Examples: Infoblox logs, Windows DNS Debug logs, BIND query logs, Splunk Stream, Bro/Zeek, Microsoft Sysmon Event 22

- Detect data exfiltration via DNS.
- Detect communication to odd/malicious domains.
- Detect communication to DGA'd domains.
- Detect communication to known Dynamic DNS domains.
- Detect shadow IT via name resolution to provisioning sites for those services.

DATA SOURCES: DNS query logs from the sources listed above and more

APPS: Core, SSE, ES, InfoSec App, UBA

Global Logon

Log on with your Global Logon Password or choose another method from the options below.

Logon Options ▾

UserID

Password

RSA Token

[Forgot Password?](#)

Remember me and use Global Logon password as my default selection

Log on

New here? [Register a password](#)

Having issues? [Return to legacy Global Logon.](#)

A phishing page ([helpdesk-att\[.\]com](https://helpdesk-att[.]com)) targeting AT&T employees. Image: urlscan.io

Need help? Visit [FAQs](#)

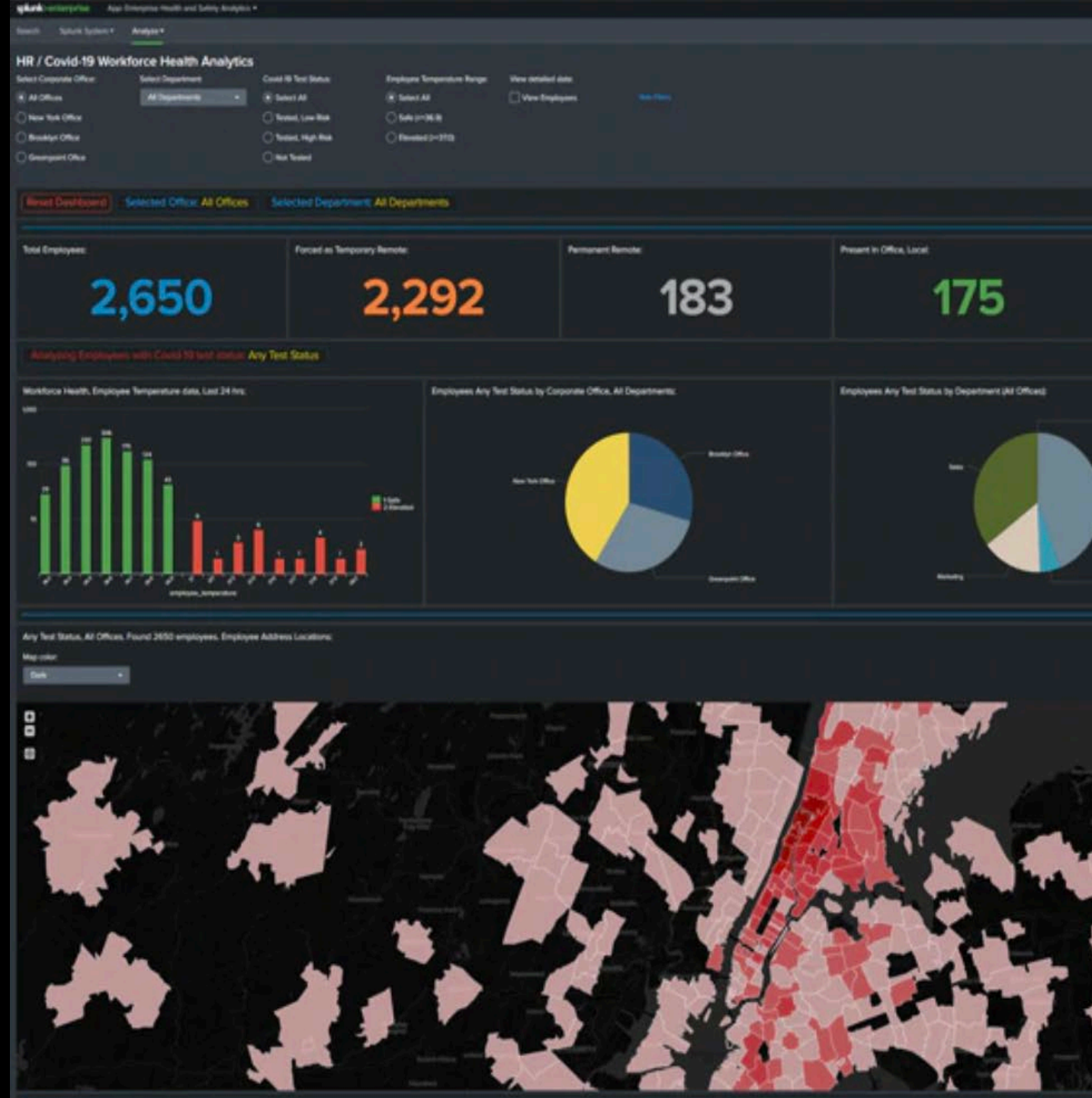
.conf20

splunk>



BOTS Example – DNS? or SSE Example Typosquatting

Physical Prem
data tells you if
people are
where they
should be!



7. Physical Premises Data Examples: Per-transaction Data From Badge Readers, Camera Activity

- Determine if you have any unauthorized entry to offices during shelter-at-home directives
- Ensure that the people entering the building are authorized
- Look for unusual camera activity
- Track the whereabouts of critical staff (execs, security personnel, etc)
- Contact tracing potential
- Support return to work activity

APPS: Core, UBA

**Web Conf &
Collaboration**
can be very
important...



8. Web Conferencing & Other “SaaS” Collaboration App Examples: Zoom, Slack, Webex, Teams, Dropbox, SFDC, ServiceNow, Workday, etc.

- Which users are using the apps, how often, where from, are you licensed
- What services within the apps are being used
- Unusual activity patterns (logins to these services from strange countries or devices)
- Evidence of “Zoombombing” trackable to rogue users
- Data exfil from SaaS apps
- Use of SaaS apps for personal use
- Use of SaaS apps from BOYD devices

DATA SOURCES: Any SaaS app with webhook, API or log access: Zoom, Slack, SFDC, Servicenow, O365, Dropbox, etc...

DATA MODEL: Web Conferencing, Authentication

APPS: Core, SSE, ES, UBA, various Splunkbase apps, Remote Work App

.conf20

splunk>

BOTS Example – Zoom TA Data or Teams Dashboard





**Do you
splunk
your
Call
Center?**

9. Ticketing Apps/Call Center Data: ServiceNow, Remedy, etc. to Find Evidence of Social Engineering

- Unusual volumes of tickets opened by users/roles
- Unusual credential resets
- Phone calls into a call center where caller ID does not match known number/work location

DATA MODELS: Ticket Management

APPS: Core, ES, SSE

.conf20

splunk>



BOTS Example Ticketing Data or – WSJ Breach Example About Password Resets



**What
about
WiFi
Data?**

10. Wireless History Data Examples: Collect History of SSIDs, MAC Addresses of Base Stations From Endpoints

- Match historical SSID with known-common SSIDs like Starbucks, ATT, hotel chains to get a rough idea of where laptop was when
- Match historical SSID with “Wigle.net” to determine precisely where a laptop is at any point in time - “Is that employee really working from home?”

DATA SOURCES: Microsoft Windows registry or scripted input collected with Universal Forwarder

APPS: Core

.conf20

splunk>



EXAMPLE – Scripted Input Data from BOTS

Are we
patched?



11. Vuln Data and Patch Data Examples: Tenable Nessus, Qualys, Rapid7, IP360, Windows Update logs, BigFix, Tanium

- Determine if your VPN infrastructure has any known vulnerabilities that could allow for adversary access
- Find unpatched endpoints accessing corporate network via VPN
- Scan endpoints over VPN to determine characteristics (unauthorized devices?)

DATA SOURCES: API or syslog vuln scan/operation data, patch data from Ufs

DATA MODELS: Vulnerability, Updates

APPS: Core, SSE, ES, InfoSec App

**What
assets
are out
there?**



12. Asset (Hardware/Software inventory), Identity Data Examples: CMDB, LDAP, Scripted Inputs, Cisco NVM, Palo Alto FW UserID, BigFix, Tanium, etc.

- Understand if authorized devices are connecting to the network
- Identify rogue/unauthorized devices connecting to the network
- Identify out-of-support versions of software being used
- Identify unauthorized hardware (USB devices) being connected.
- Find vulnerable versions of software.
- Map usernames to roles/location/asset.

DATA SOURCES: ServiceNow, OSquery, various endpoint tech, Palo Alto UserID, various VPN tech

APPS: Core, SSE, ES, InfoSec App, UBA

.conf20

splunk>

BOTS Example – Security Training Confirmation





Take-aways!

- There are many different security concerns that require renewed focus in this WFH world
- Splunk can help you make the most of ~12 different data sources so that you're covering most of these concerns
- Rely on the resources at this link to help!

https://splk.it/conf20_wfh_sec



Thank You

Please provide feedback via the

SESSION SURVEY

