



TOP CYBER PHENOMENA EMERGING FROM THE PANDEMIC

Ron Meyran

Director, Security Solutions

November 18, 2020



When COVID-19 Started...

ORGANIZATIONS FOCUSED ON SCALING CAPACITY & MAINTAINING SERVICE AVAILABILITY

ENABLE
Expansion

ENSURE
Availability

September 23, 2020 | Topic: Technology | Blog Brand: Techland | Tags: COVID-19, Coronavirus, Pandemic, Technology, Laptop, School

Trying to Buy a Laptop? COVID-19 Is Creating a Shortage.

Students are back in school, and in much of the country, they're still learning remotely. That, along with the many professionals who are continuing to work from home, led to a significant run on laptops, whether they were being purchased by parents individually, or by school districts in bulk.

by Stephen Silver



1

Accelerated Digital Transformation

APPLICATIONS/SERVICES ARE GOING DIGITAL & CLOUD

Cloud Migration, automation, and the streamlining of processes helped organizations weather the economic storm that resulted from COVID-19

76%

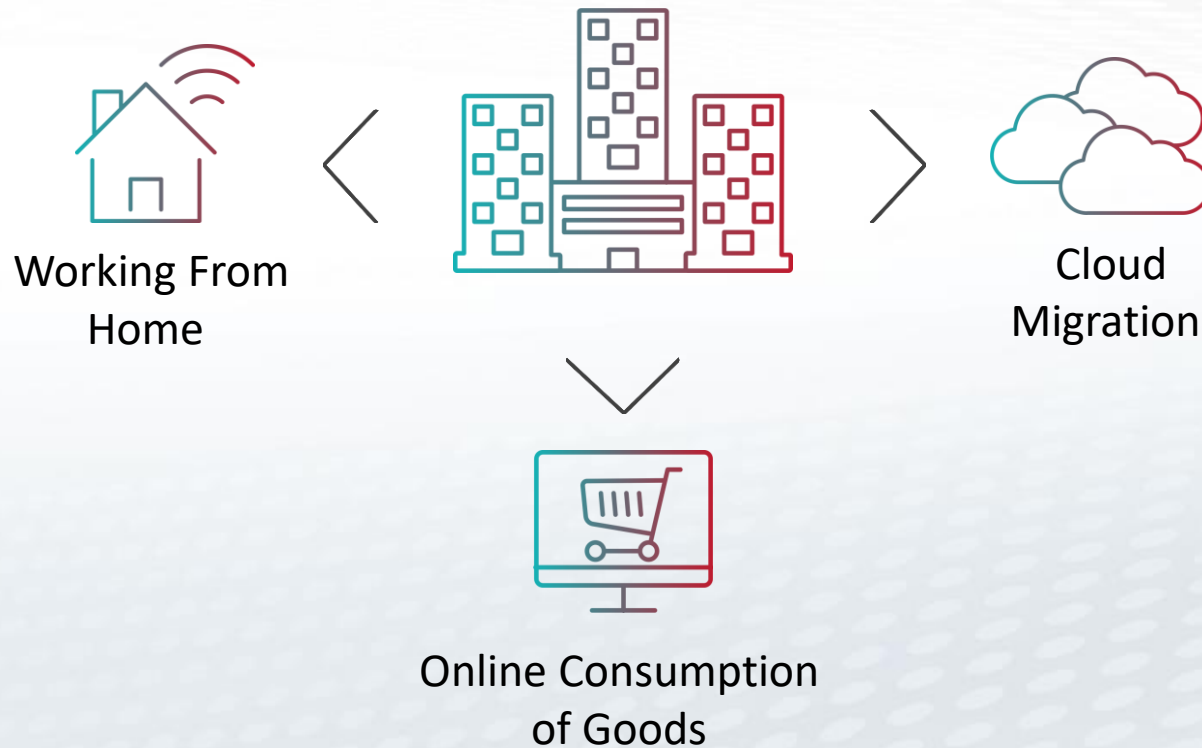
OF THE RESPONDENTS
SAID THAT THE PANDEMIC
**ACCELERATED THEIR PLANS
FOR CLOUD MIGRATION.**

56%

OF COMPANIES WITH INTERESTS
IN ONLINE ORDERING, HOME
DELIVERY, TELECONFERENCE AND
STREAMING SERVICES **FOCUS ON
NEW REVENUE MODELS.**

2

Evolving Threat Landscape



APPROXIMATELY

50%

of the respondents were not confident in their organizations' ability to effectively protect against unknown threats.

30%

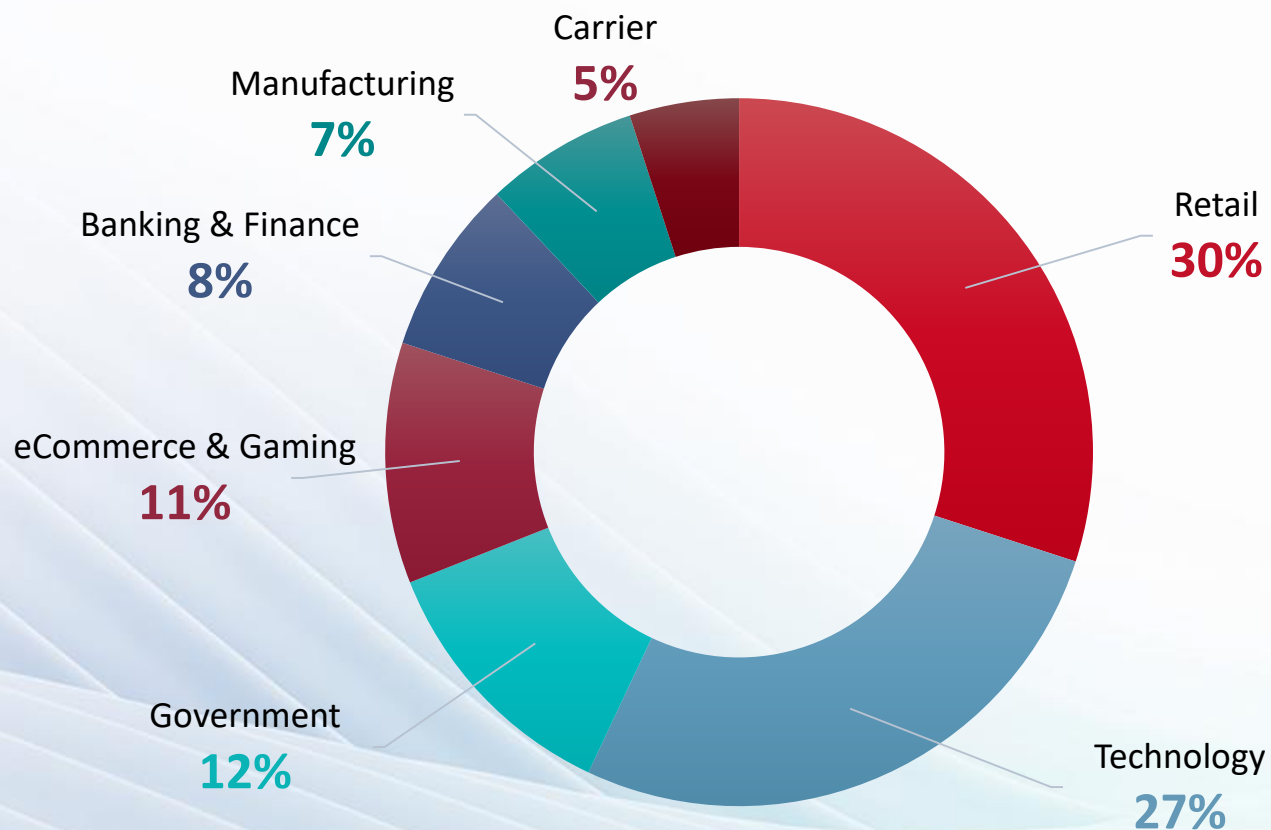
Reported an increase in attacks after the onset of the COVID-19 pandemic.

RESULT: MORE OPPORTUNITIES FOR ATTACKERS TO LEVERAGE

3

Growing Trend of Attacks on Financial Services & eCommerce

TOP ATTACKED VERTICALS



* Global attacks insight, October 2020, Radware Cloud Services

+1B bad bot requests
detected per month*

163K Total DDoS
Attacks Blocked

1.7TB Total DDoS Attacks
Volume Blocked

53 Volumetric DDoS Attacks
Blocked (>10Gbps):

160M Total Web Application
Attack Transactions Blocked

* In Q3'20



Actors & Motives



ORGANIZED CRIME



ANGRY USERS



HACKTIVISTS



COMPETITORS



SCRIPT KIDDIES



NATION STATES

Global Ransom DDoS Campaign

TARGETING FINANCE, TRAVEL AND E-COMMERCE

Cyber Security Review

News • Insights • Analysis

About the Review News Articles Events Editorial **Subscribe** Resources Contact



Tag: Brazil

Brazil's court system under massive RansomExx ransomware attack

November 5, 2020

Brazil's Superior Court of Justice was hit by a ransomware attack on Tuesday during judgment sessions that were taking place over video conference. "The Superior Court of Justice (STJ) announces that the court's information technology network suffered a hacker attack [Read More ...](#)

News November 2020 Cybercrime, Ransomware, Threat Intelligence, Brazil, TTP, Judiciary, RansomExx ransomware

Subject: DDoS Attack on [REDACTED]

We are the Lazarus Group and we have chosen [REDACTED] as target for our next DDoS attack.

Please perform a google search for "Lazarus Group" to have a look at some of our previous work.

Your whole network will be subject to a DDoS attack starting at [REDACTED] next week. (This is not a hoax, and to prove it right now we will start a small attack on your [REDACTED] servers that will last for about 1 hour. It will not be heavy attack, and will not cause you any damage, so don't worry at this moment.) There's no counter measure to this, because we will be attacking your IPs directly (AS [REDACTED]) and our attacks are extremely powerful (peak over 2Tbps)

What does this mean? This means that your websites and other connected services will be unavailable for everyone. Please also note that this will severely damage your reputation among your customers. Will [REDACTED] at [REDACTED] even be possible? You can wait to see.

How can you stop this? We will refrain from attacking your servers for a small fee. The current fee is 20 Bitcoin (BTC). It's a small price for what will happen when your whole network goes down. Is it worth it? You decide!

We are giving you time to buy Bitcoin if you don't have it already.

If you don't pay attack will start, fee to stop will increase to 30 BTC and will increase by 10 Bitcoin for each day after deadline that passed without payment.

Please send Bitcoin to the following Bitcoin address: [REDACTED]

Once you have paid we will automatically get informed that it was your payment.

Please not that you have to make payment before the deadline or the attack WILL start!

What if you don't pay?

If you decide not to pay, we will start the attack on the indicated date and uphold it until you do. We will completely destroy your reputation and make sure your services will remain offline until you pay.

Do not reply to this email, don't try to reason or negotiate, we will not read any replies.

Once you have paid we won't start the attack and you will never hear from us again. Please not that no one will find out that you have complied



DDoS Attacks on Gaming – Oct 2020





FBI Warning: Account Take Over Attacks

TLP:WHITE

Private Industry Notification

FEDERAL BUREAU OF INVESTIGATION



10 September 2020

PIN Number
20200910-001

Please contact the FBI with any questions related to this Private Industry Notification at either your local **Cyber Task Force** or **FBI CyWatch**.

Local Field Offices:
www.fbi.gov/contact-us/field

E-mail:

The following information is being provided to you under the Freedom of Information Act (FOIA) exemptions, for potential recipients to protect against cyber threats. This information was coordinated with CISA and the FBI.

This PIN has been released **TLP:WHITE** rules, **TLP:WHITE** information may be released.

Cyber Actors Conduct Credential Stuffing Attacks Against US Financial Institutions

This notification was created jointly by the FBI and the Investigative Joint Task Force (NCJTF).

Summary

Since 2017, the FBI has received numerous reports of credential stuffing attacks^a against US financial institutions. These attacks involve the use of stolen credentials to gain unauthorized access to financial services providers, insurance companies, and other critical infrastructure. During this timeframe, the FBI has

ZDNet

MUST READ: Trade war restrictions force Huawei to sell off Honor business

Brute-force cyberattacks on the rise in Brazil

The widespread adoption of remote working is the main driver behind the increase, according to a new report.

Close More Deals Remotely

[Book A Demo](#)

[Refract](#)

By Angelica Mari | August 24, 2020 -- 18:00 GMT (19:00 BST) | Topic: Security

Brazil has seen a spike in brute-force cyberattacks driven by the increase in remote working, according to a new report on security threats in the first six months of 2020.

More than 2.6 billion attempts at cyber attacks have been recorded by cybersecurity firm Fortinet from January to June, out of a total of 15 billion attempts across Latin America and the Caribbean.

According to the report, there has been a "considerable increase" of brute-force attacks - the practice of guessing possible combinations of login information multiple times through automated means, until the correct access information is discovered.

The increase in the uptake of remote working has rekindled the interest of cybercriminals in this type of attack, according to Alexandre Bonatti, Engineering Director at Fortinet Brazil: "[Attackers] are finding a significant number of incorrectly configured Remote Desktop Protocol servers, which facilitates invasions," he noted.

Never Old.
Never Never.



* Source: <https://www.documentcloud.org/documents/7208239-FBI-PIN-on-credential-stuffing-attacks.html>



Top Cyber Phenomena Emerging from the pandemic



ACCELERATED DIGITAL TRANSFORMATION

Applications/Services are going
Digital & Cloud



EVOLVING THREAT LANDSCAPE

Organizations' attack surface
increases due to changing
economy



GROWTH OF ATTACKS VOLUME

Trend of Attacks on Financial
Services, eCommerce & gaming



Accelerated Digital Transformation. SECURED.

DON'T LEAVE SECURITY BEHIND AS YOU SHIFT TO THE CLOUD

ENABLE

Expansion

ENSURE

Availability

PROTECT

Infra & Apps

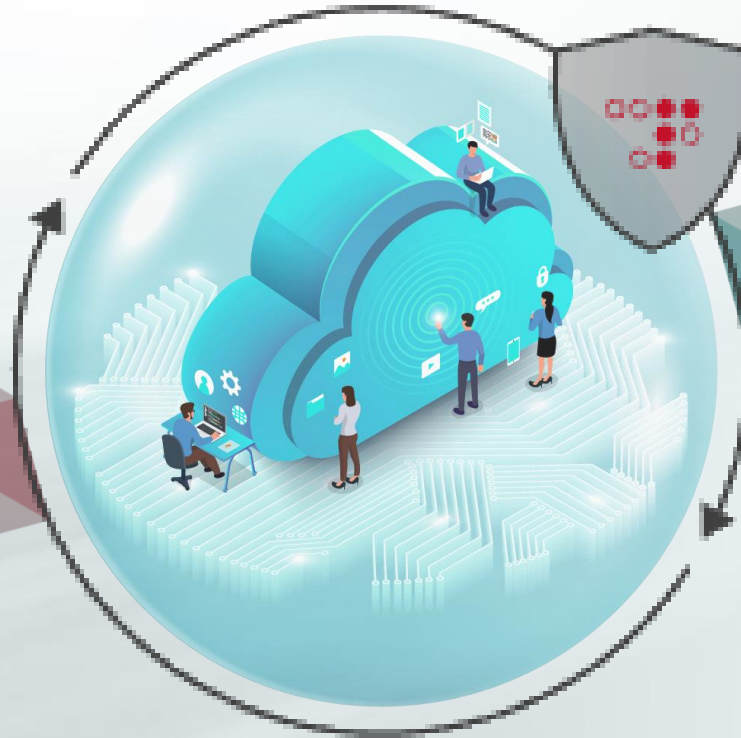
SECURE

Cloud
Environments

Need for HOLISTIC Security Protection

PROTECT INFRA & APPS

- ✓ WEB APP ATTACKS
- ✓ L3-7 DDOS
- ✓ BAD BOTS
- ✓ API ABUSE



SECURE CLOUD ENVIRONMENTS

- ✓ PUBLICLY EXPOSED ASSETS
- ✓ MISCONFIGURATIONS
- ✓ PRIVILEGE ESCALATION
- ✓ CREDENTIAL ABUSE

PROTECT YOUR INFRA & APPS ACROSS MULTI ENVIRONMENTS



HOW TO SECURE YOUR DIGITAL TRANSFORMATION

1

COVER **ALL** ATTACK SURFACES

Application surface and infrastructure

2

PUBLIC CLOUD THREATS ARE **DIFFERENT**

Cloud-specific protections are needed

3

PROTECTION FOR **EVERY** ENVIRONMENT

Protect your cloud transition and mixed environments

Thank You!