HOW CYBERCRIMINALS TOOK ADVANTAGE OF COVID-19

In the advent of one invisible threat, another took form in 2020.

No other event has gripped the planet so much in the digital age. As many isolated, worked from home, and waited for information, cybercriminals went on the attack at an intensity never seen before.

THE PANDEMIC BECOMES A CRIMINAL OPPORTUNITY

400% increase in cyberattacks

FBI CYBER DIVISION SEES AN INCREASE of daily cybercrime complaints to 4,000 a day during COVID-19 compared to the previous year.[1]

PHISHING WITH COVID-19 AS BAIT is so effective that Microsoft reports that this is being done tens of thousands of times a day.[2]

30,000 COVID-19 themed attacks per day

1 OUT OF 5 phishing emails blocked

GOOGLE IS BLOCKING MILLIONS OF PHISHING EMAILS every day – of the 100 million blocked daily, 18 million use COVID-19 as their lure.[3]

NO INDUSTRY WAS SPARED

HEALTHCARE
Eight Magellan Health entities and approximately **365,000 PATIENTS** were breached by a socially engineered **phishing attack.**[4]

FINTECH
Finastra, which supplies software to **90% OF THE WORLD'S TOP 100 BANKS,** withstood a **ransomware attack** of key systems that went unnoticed for three days.[5]

COMMUNICATION TECHNOLOGY
A list of **500,000 ZOOM USER ACCOUNTS** and passwords were obtained using **credential stuffing.**[6]

GLOBAL FINANCE
The New Zealand Stock Exchange went offline for 2 days as its network was compromised by a **DDoS attack.**[7]

EDUCATION
Educational resources are under intense strain compared to 2019, with **DDoS attacks** affecting resources by an additional **350% IN 2020.**[8]

SOCIAL MEDIA
The Twitter accounts of several high-profile figures, including Joe Biden, Elon Musk, Bill Gates, and Barack Obama, as well as the brand handles for Apple and Uber, were accessed with the use of **social engineering** promising followers a chance to to promote a bitcoin scam [9]

GOVERNMENT
Cyberattacks on state and local governments rose by **50%, WITH RANSOMWARE** demands increasing to up to nearly half a million dollars.[10]

Multiple U.S. federal networks and major corporations such as Cisco, Intel, and many more were infected when cybercriminals hacked and piggybacked on **SOLARWINDS SOFTWARE UPDATES** to spy and move through networks undetected for months.[11]

THE COST OF CYBERCRIME

$6 TRILLION
Estimated global cost of cybercrime in 2021[12]

$20 BILLION
Estimated global cost of ransomware attacks in 2021[13]

$5.86 MILLION
Average cost of a data breach in the fintech industry[14]

$3.86 MILLION
Average cost of a data breach[15]

TOP CYBERSECURITY CONCERNS

Society is evolving as we navigate through this pandemic. There is an increased demand for solutions that allow us to do "anything from anywhere." This has led to wider adoption of digital mediums and services for accessing information and conducting transactions. In parallel, cybercriminals are also ramping up and changing their attack vectors, causing larger business disruption and massive financial losses.

42% OF THE U.S. WORKFORCE IS WORKING FROM HOME, with many of those jobs remaining remote for the unforeseen future.[16]

69% OF IT DECISION MAKERS ARE CONCERNED with work-from-home (WFH) security risks, like insecure networks, use of personal devices, data leakage, and low user awareness.[17]

80% OF DATA BREACHES ARE DUE TO COMPROMISED, weak, and reused credentials, such as passwords.[18]

7X INCREASE IN RANSOMWARE attacks in 2020 compared to the previous year, making ransomware the go-to mechanism for hackers.[19]

57% OF DEVICES VULNERABLE TO ATTACKS[20] and an estimated 31 billion devices expected to be connected in 2020[21] – IoT is the low-hanging fruit for cybercriminals.

4 MILLION UNFILLED CYBERSECURITY JOBS worldwide by 2021 adds to the challenge of securing data and identities.[22]

IT

ENTRUST IDENTITY: A PERFECT DEFENSE

Any defense against invisible threats must be intelligent and built to adapt to attacks that can take on any number of forms, or be deployed by any number of methods. Entrust Identity is the identity and access management (IAM) portfolio that provides the strong foundation needed to protect your workforce, consumers, and citizens.

Entrust Identity for Workforce

High assurance authentication with certificate based credentials
Zero Trust approach
MFA with passwordless access + SSO
Easy integrations across apps, portals, and enterprise platforms
Risk-based adaptive authentication

Entrust Identity for Consumers

Biometric enabled authentication for a passwordless experience
Strong customer authentication with industry-best MFA
Self-service identity issuance (identity proofing)
User-friendly password reset
Omnichannel experience – all devices, apps + mobile SDK to embed and brand as your own

Entrust Identity for Citizens

Digital travel credentials, mobile driving licenses, national ID, student ID
Seamless integration with government agencies (platform, websites, and portals)
Collaborates with government-selected contractors for all IAM needs

ENTRUST
SECURING A WORLD IN MOTION

SOURCES:

1 - "FBI sees spike in cyber crime reports during coronavirus pandemic", April 2020, The Hill

2 - "Exploiting a crisis: How cybercriminals behaved during the outbreak", June 2020, Microsoft

3 - "Google blocking 18m coronavirus scam emails every day", April 2020, BBC

4 - "Magellan Health Data Breach Victim Tally Reaches 365K Patients", July 2020, Health IT Security

5 - "Fintech Company Survived Ransomware Attack Without Paying Ransom", April 2020, Bloomberg

6 - "Zoom Gets Stuffed: Here's How Hackers Got Hold of 500,000 Passwords", April 2020, Forbes

7 - "New Zealand stock exchange halted by cyber attack", August 2020, BBC

8 - Kaspersky Digital Education: The cyberrisks of the online classroom, April 2020

9 - "Twitter's massive attack: What we know after Apple, Biden, Obama, Musk and others tweeted a bitcoin scam", July 2020, The Verge

10 - "Cyberattacks on state, local government up 50%", September 2020, GCN

11 - "Why the US government hack is literally keeping security experts awake at night", December 2020, CNN

12 - "Cybercrime To Cost the World $10.5 Trillion Annually By 2025", November 2020, Cybercrime Magazine

13 - "Global Ransomware Damage Costs Predicted To Reach $20 Billion (USD) By 2021", October 2019, Cybercrime Magazine

14 - "What is the cost of a data breach?", August 2020, CSO

15 - IBM Cost of Data Breach Report 2020

16 - "Stanford research provides a snapshot of a new working-from-home economy", June 2020, Standford News

17 - "New Research Indicates 84% of Businesses Will Likely Increase Work-from-home Capacity Beyond Pandemic Despite Security Concerns", May 2020, PulseSecure

18 - Verizon 2020 Data Breach Investigations Report

19 - Bitdefender Mid-Year Threat Landscape Report 2020

20 - Palo Alto Networks 2020 Unit 42 IoT Threat Report

21 - "The IoT Rundown for 2020: Stats, Risks and Solutions", January 2020, Security Today

22 - "Bridging the Cybersecurity Skills Gap", June 2020, Netsparker