# Cybersecurity

## Maryland Government Finance Officers Association

Andrew Hartridge
Chief Information Security Officer
M&T Bank
February 18, 2022



M&T Tech

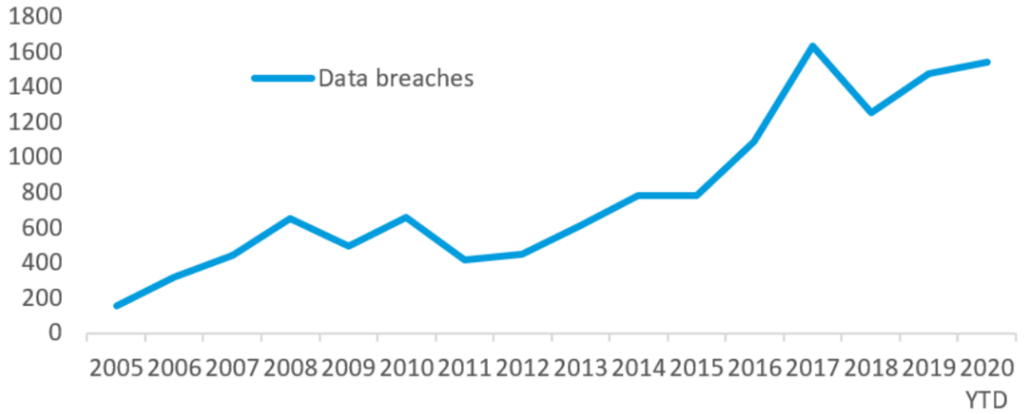
# Background

How large is the cybersecurity crime landscape?

- One of the biggest threats to businesses/agencies of all sizes is cyber crime
- Why would a cybercriminal target your business/agency?
  - You have what they want
    - Personal information
    - Financial Theft/Fraud
    - Employee information
    - Medical records
  - Politically Motivated Disruption
  - Vigilantism

**Threats rising**

Explosion in cyber attack incidents.




Source: Identity Theft Resource Center.



M&T Tech

# Types of Attacks and Threats

- Attack Examples:
  - Ransomware
  - Phishing/Smishing/Vishing
  - Distributed Denial of Service (DDoS)
  - Fraudulent Transactions
  - Theft of Intellectual Property
  - Vandalism
  - Personal/Agency Embarrassment
  - Manipulation of Industrial Systems

**Internal Threats**

Employees Vendors

- Malicious: stealing information (e.g. stealing customers information, card skimming)
- Negligence: lost resources storing information (e.g. laptops, smartphones, tablets)

**External Threats**

Individual Threat Actors | Hacktivists | Organized Criminals | Nation-state

- Steal information
- Utilize viruses or malicious code
- Disrupt businesses via cyber vandalism
- Pursuing social or political agenda

# Ransomware

## What is Ransomware?

- A computer program designed to block access (often by encrypting it) to systems and data until a sum of money is paid
- Ransomware criminals often target and threaten to sell or leak stolen data or important information if the ransom is not paid

## How?

- Modern criminals target valuable data from an organization, and often exfiltrate it rather than encrypt it
- Usually started by phishing emails and software flaws
- A tactic involving the use of a malicious software (also known as malware) that, when downloaded to a computer, encrypts files so they can no longer be accessed — or it locks down the operating system entirely so the user can no longer access anything

# Credential Re-Use

- An unfortunate trend where customers/constituents re-use the same username and password on multiple sites
- Threat actors obtain username and password combinations from various breaches
- They use tools to automatically log in using the stolen credentials to see where they work, and ultimately commit fraud or sell the information
- 80% of hacking-related breaches involved weak or stolen credentials
- Quick defense tips:
    - Change default credentials
    - Use different passwords across multiple online sites

# Phishing/Smishing/Vishing

## Social Engineering

- The use of deception to manipulate individuals into divulging confidential or personal information that may be used for fraudulent purposes.

## Phishing

- A tactic involving the use of a fraudulent email to trick the recipient into opening a malicious attachment or visiting a malicious website.
- The goal is to have you divulge sensitive information or provide an avenue for the hacker to steal your credentials

## Smishing

- The fraudulent practice of sending a test message stating to be from a reputable company in order to gain personal information from an individual

## Vishing

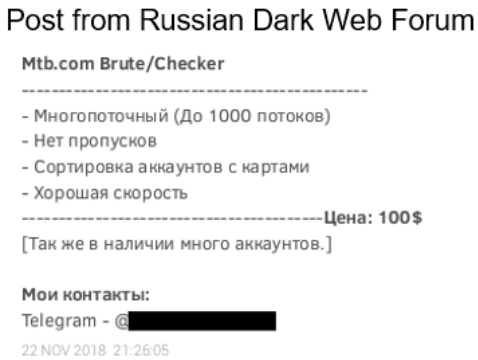
- The fraudulent practice of making phone calls or leaving voice messages stating to be from a reputable company in order to gain personal information from an individual

# Distributed Denial of Service (DDoS)

- A DDoS attack is a malicious attempt to disrupt the normal traffic of a targeted server, service or network by overwhelming the target
- These attacks achieve effectiveness by utilizing multiple compromised computer systems
- Attacks are carried about by networks that have been infected with malware, allowing them to be controlled remotely by an attacker

# Credential Re-Use Example

- Definition: Credential re-use is a cybersecurity attack in which credentials obtained from a data breach on one service are used to attempt to log in to another unrelated service.
- Credential Stuffing Example: Threat Actor Post for credential re-use tool:


Post from Russian Dark Web Forum

**Mtb.com Brute/Checker**

---

- Многопоточный (До 1000 потоков)
- Нет пропусков
- Сортировка аккаунтов с картами
- Хорошая скорость

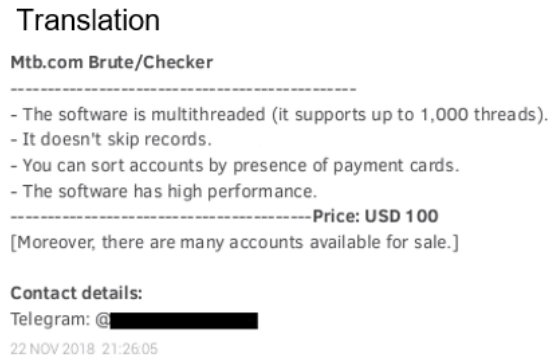
----------**Цена: 100$**

[Так же в наличии много аккаунтов.]

**Мои контакты:**

Telegram - @[redacted]

22 NOV 2018 21:26:05


Translation

**Mtb.com Brute/Checker**

---

- The software is multithreaded (it supports up to 1,000 threads).
- It doesn't skip records.
- You can sort accounts by presence of payment cards.
- The software has high performance.

----------**Price: USD 100**

[Moreover, there are many accounts available for sale.]

**Contact details:**

Telegram: @[redacted]

22 NOV 2018 21:26:05



M&T Tech

# Phishing & Smishing Examples

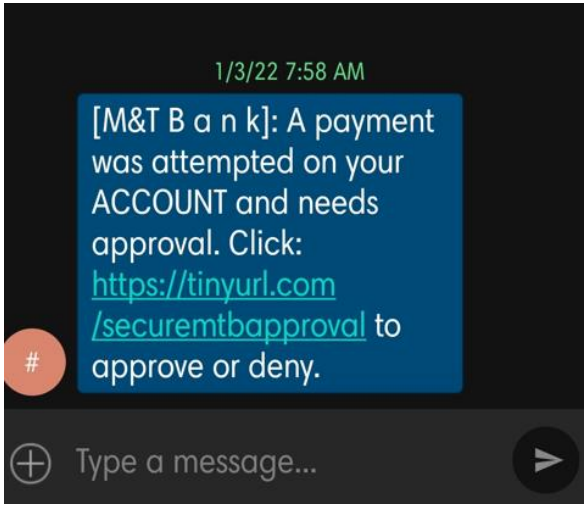

DOCUMENT

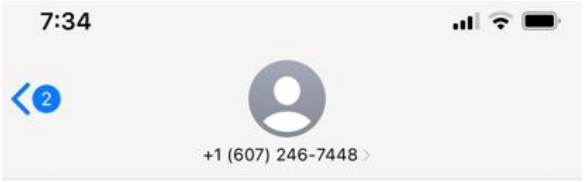
Notification from Corporate site.

**Documents**

| Document Name | Received Date |
|---|---|
| KB213 2022-0010 | 01/18/2022 |

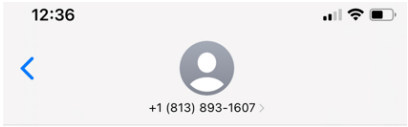
CLICK HERE TO VIEW DOCUMENT




Text Message
Today 7:22 AM

M&T Bank: Your One Time Passcode is 598267. Do not share this passcode with anyone. If you did not request for this code, verify as follows now to avoid fraudulent activities on your account. Verify now at https://onlinecity.co.in/mtb/



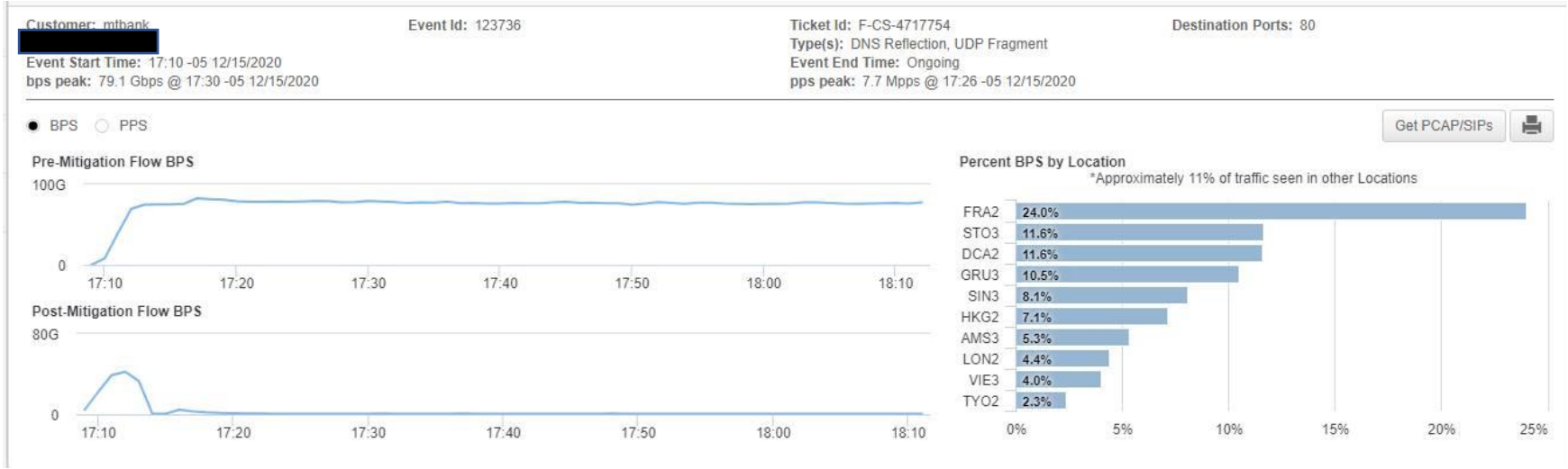

Text Message
Today 11:49 AM

M&T :ONLINE SERVICE LOCKED! SUSPICIOUS ACTIVITIES DETECTED. VERIFY IDENTITY IMMEDIATELY AT https:// vrili31check-my-mtb.com TO REGAIN ACCESS.



M&T Tech

# DDoS Example






M&T Tech

# Risk Reduction

## How to protect yourself and your agencies

- Increased Cybersecurity conversations
- Protect your “Digital Identity”
- Keep your software and operating system up-to-date with appropriate off-site backup
- Security awareness for all employees
- Work with internal and external IT professionals to develop and exercise Incident Response plans

The best advice for all audiences?

**Think before you click!**

43% of cyberattacks are aimed at small businesses, but only 14% are prepared to defend themselves

## Government Assistance on Ransomware

- Cybersecurity and Infrastructure Security Agency (CISA) – StopRansomware.com
- Tech firms partnering with government agencies to fight ransomware
  - Cybersecurity & IT | Maryland is Open for Business
- If you are a victim of ransomware:
  - Follow your agency’s incident response procedures

# Cybersecurity

## Maryland Government Finance Officers Association

Andrew Hartridge
Chief Information Security Officer
M&T Bank
February 18, 2022



M&T Tech