500 MILLION BLOCKED THREAT MESSAGES: IT SECURITY UPDATE

ERNIE SOFFRONOFF
DIRECTOR, WSE IT
ERNIE.S@JHU.EDU
A BIG SCARY NUMBER!

- In 2020, 61% of email blocked at Internet border before going to mailboxes
- That’s actually down from 2017, when about 75% of email was blocked
- There are about a dozen layers of protection to traverse for email messages coming from outside JH
- Other tools to clean up threat messages that do make it through
- Ten times more blocked email than Elvis fans?
REMEMBER:

Everything discussed here as being good for Hopkins also applies to your own personal online security.
AGENDA

• Terminology
• Are the threats real?
• What are our risks?
• What should we do?
• Questions?
TERMINOLOGY
WHAT IS IT SECURITY?

• We are considering Confidentiality, Integrity, and Availability

• Not everything needs to be secure, but it’s important we understand and accept the risks of the degree of security applied

• How would you want this handled if it was YOUR information?
WHAT IS PERSONALLY IDENTIFIABLE INFORMATION?

It includes, but is not limited to:
• SSNs
• Dates of Birth
• Financial Account Information
• Driver’s License Numbers
• Credit Card Numbers
• Health Information

PII is often more sensitive in combinations than in isolation:
• Email address: not sensitive
• Last four of SSN: not (that) sensitive
• Together? Very sensitive!
ARE THE THREATS REAL?
HIGHER EDUCATION CYBER ATTACKS

Colleges a ‘Juicy Target’ for Cyberextortion

Cybercriminals using ransomware increasingly focus on colleges and universities. What steps can institutions take to minimize their own risks – and threats to the sector?

By Lindsay McKenzie // March 19, 2021
ABOUT BREACHES

Figure 2. What tactics are utilized? (Actions)

- 70% perpetrated by External actors
- Organized criminal groups were behind 55% of breaches
- 30% involved internal actors
- Only 4% of breaches had four or more attacker actions
- 1% involved Partner actors
- 1% featured multiple parties

Figure 3. Who’s behind the breaches?

- 45% of breaches featured Hacking
- Errors were causal events in 22% of breaches
- 22% included Social attacks
- 17% involved Malware
- 8% of breaches were Misuse by authorized users
- Physical actions were present in 4% of breaches

Source: Verizon 2020 Data Breach Investigation Report
MORE ABOUT BREACHES

Frequency
819 incidents, 228 with confirmed data disclosure

Top Patterns
Miscellaneous Errors and Web Applications represent 81% of breaches

Threat Actors
External (67%), Internal (33%), Partner (1%), Multiple (1%)

Actor Motives
Financial (92%), Fun (5%), Convenience (3%), Espionage (3%), Secondary (2%)

Data Compromised
Personal (75%), Credentials (30%), Other (23%), Internal (13%)

Figure 5. What are the other commonalities?

Source: Verizon 2020 Data Breach Investigation Report
MORE ABOUT BREACHES

Figure 6. Select action varieties in breaches over time

- **Malware**
  - RAM scraper
- **Social Phishing**
- **Trojan**
- **Hacking**
  - Use of stolen creds
- **Malware**
  - Password dumper
- **Error**
  - Misdelivery
- **Malware**
  - Ransomware
- **Error**
  - Misconfiguration

**Phishing** (-6.6% from last DBIR)
**Use of stolen creds** (-4.1% from last DBIR)
**Misdelivery** (1.4% from last DBIR)
**Misconfiguration** (4.9% from last DBIR)
**Password dumper** (4.2% from last DBIR)
**Trojan** (-15.4% from last DBIR)
**Ransomware** (2.6% from last DBIR)
**RAM scraper** (-1.8% from last DBIR)

Source: Verizon 2020 Data Breach Investigation Report
WHAT ARE OUR RISKS?
Dear Colleagues:

Members of the Johns Hopkins community are being targeted by a phishing email appearing to be from Johns Hopkins IT. It asks you to click a link to view your account status.

This link takes you to a fake page intended to trick you into providing your login and personal information.

This is the latest in a series of phishing scams intended to deceive people into responding to an official Johns Hopkins request. To protect your personal information and the security of Johns Hopkins' systems, please be extremely cautious about clicking any links or responding to any emails.

Know what to look for

The new phishing email looks like this screenshot:

From: JHED IT [mailto:jhedsupport@comcast.net]
Sent: Wednesday, January 18, 2017 1:23 PM
Subject: Secure Validation

Michelle Thompson
Equifax/TAX W2
To: 

Dear Liaisons:

As we discussed in a recent meeting, Hopkins is sending out letters to individuals that have either self-reported 2017 tax fraud or for whom we have identified potential fraud through our Equifax/TAX W2 service. You may have questions about this in your organization. Answer each question below. In a few weeks, Wanda will contact your organization if your questions are not resolved.

Late Wednesday, a firm working with a firm in spring (under the signatures of University personnel but also others) asked you to follow a link and enter your login or personal information.

For questions or concerns, please:

1) You should first direct them to IDEX Experts. IDEX Experts is able to efficiently assist you, 999-4170.

2) If the caller insists on talking to the address below (even if the address provided is incorrect), they contact IDEXExperts. For more information, please contact the office: tax.office@jhu.edu

3) If you or another administrative assistant receive a call, please try to avoid answering the call and be for the next available.

4) Some people may try to call your phone number. The phone number may not be able to access your account.

5) If you have questions, please call the address below.

Thanks.

January 27, 2021

Dear Johns Hopkins Faculty and Staff,

It’s the time of year when preparing to file 2020 income taxes becomes top of mind, and we have important updates and information to share with you.

Be aware of scams

We’d like to remind you to please be aware of scams involving W-2s, tax filing, and your personal information. To avoid being the victim of a scam, please be aware of the following:

- Consider filing your taxes as early as possible, because the IRS allows only one tax return per individual per year.

Thank you for your attention to these matters.

Sincerely,

Johns Hopkins University
WHITING SCHOOL OF ENGINEERING
CRYPTOLOCKER? WANNACRY?

Ooops, your files have been encrypted!

What Happened to My Computer?
Your important files are encrypted.
Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

Can I Recover My Files?
Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.
You can decrypt some of your files for free. Try now by clicking <Decrypt>.
But if you want to decrypt all your files, you need to pay.
You only have 3 days to submit the payment. After that the price will be doubled.
Also, if you don’t pay in 7 days, you won’t be able to recover your files forever.
We will have free events for users who are so poor that they couldn’t pay in 6 months.

How Do I Pay?
Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.
Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.
And send the correct amount to the address specified in this window.
After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am GMT from Monday to Friday.

Send $300 worth of bitcoin to this address:

12t9YDPgwueZ9NyMgw519p7AA8isj6SMw

Copy

Check Payment

Repeat
DISCLOSURE NOTIFICATION

Johns Hopkins Statement: Breach of Biomedical Engineering Office Database

March 7, 2014
FOR IMMEDIATE RELEASE
CONTACT: Dennis O’Shea
443-997-9912 (office)
410-496-7460 (cell)
dros@jhu.edu

The following statement may be attributed to Johns Hopkins University spokesmen:

Johns Hopkins has learned from the FBI that information stolen from a Department of Biomedical Engineering database had been posted on the Internet on Thursday, March 6. This came one day after the discovery of an extortion message from someone claiming to be a member of the hackers’ group.

The extortionist threatened to post stolen BME Department data if the university did not not provide the hackers’ demands.

The department, the Whiting School of Engineering and the university are working with the FBI’s criminal investigation. We are still gathering information, but here is what we know:

The server in question is used primarily to produce the Biomedical Engineering Electronic Media database. It is used to store and distribute images, videos, and other multimedia content.

— The server in question is used primarily to produce the Biomedical Engineering Electronic Media database. It is used to store and distribute images, videos, and other multimedia content.

— The server in question is used primarily to produce the Biomedical Engineering Electronic Media database. It is used to store and distribute images, videos, and other multimedia content.

— The server in question is used primarily to produce the Biomedical Engineering Electronic Media database. It is used to store and distribute images, videos, and other multimedia content.

— There is no evidence that the database on the server contained Social Security numbers or other personally identifiable information.

Maryland Information Security Breach Notices

As of January 2008, any business that retains consumer records is required by Maryland law to notify a consumer if his or her information is compromised. The "security breach law" also requires the Business Attorneys General to list on their websites information security breach notices sent to the OAG from 2017 to the present. Questions about specific notices may be directed to IDTheft@oag.state.md.us. Below is a chart containing the case number, date of the notice, business name, and number of Maryland residents affected by the breach.

<table>
<thead>
<tr>
<th>Case Title</th>
<th>Case No.</th>
<th>Date Received</th>
<th>No of MD Residents</th>
<th>Information Breached</th>
<th>How to Report</th>
</tr>
</thead>
<tbody>
<tr>
<td>World Vision, Inc.</td>
<td>3331763</td>
<td>8/31/2020</td>
<td>4</td>
<td>name, contact information, email, physical mailing address, ssn driver license number, financial account information, and date of birth</td>
<td>ran out of space</td>
</tr>
</tbody>
</table>
WHAT SHOULD WE DO?
1. Implement a Security Awareness and Training Program
2. Boundary Defense
3. Secure Configuration – PLEASE REBOOT WEEKLY

NEW: MyLearning “JHU Electronic Information Security and Data Management”
<table>
<thead>
<tr>
<th>Problem</th>
<th>Responses</th>
</tr>
</thead>
</table>
| Phishing (or other threat) Email | • Healthy skepticism  
• Look for traits of “real” login page  
• Forward messages to spam@jhu.edu  
• Don’t use external mailbox (Gmail) for work email |
| Stolen Credentials            | • Multi-factor authentication  
• Don’t reuse passwords  
• Password rotation, password quality  
• Notifications on account activity |
| Malware and Cryptolocker      | • Keep patches up to date  
• Back up files to server, or use desktop backup  
• Use OneDrive  
• Be mindful of what networks you connect to |
| Information Disclosure        | • Minimize retained data in scope and time  
• Encryption for devices  
• Share data using OneDrive, [secure] email service  
• Hygiene for your desk (shred papers, lock workstation) |
CAN YOU LIMIT WHAT DATA COULD BE LEAKED?

From this:

<table>
<thead>
<tr>
<th>Name</th>
<th>JHED</th>
<th>Birthdate</th>
<th>SSN</th>
</tr>
</thead>
<tbody>
<tr>
<td>Person, Newest</td>
<td>nperson7</td>
<td>August 19, 1999</td>
<td>012-34-5678</td>
</tr>
<tr>
<td>Person, Middle</td>
<td>mperson4</td>
<td>March 25, 1985</td>
<td>876-54-3210</td>
</tr>
<tr>
<td>Person, Oldest</td>
<td>operson1</td>
<td>June 5, 1970</td>
<td>123-45-6789</td>
</tr>
</tbody>
</table>

To this:

<table>
<thead>
<tr>
<th>Name</th>
<th>JHED</th>
<th>Birthdate</th>
<th>SSN</th>
</tr>
</thead>
<tbody>
<tr>
<td>Person, Newest</td>
<td>nperson7</td>
<td>(redacted)</td>
<td>5678</td>
</tr>
<tr>
<td>Person, Middle</td>
<td>mperson4</td>
<td>(redacted)</td>
<td>3210</td>
</tr>
<tr>
<td>(redacted)</td>
<td>(redacted)</td>
<td>(redacted)</td>
<td>(redacted)</td>
</tr>
</tbody>
</table>