eCommerce Security during COVID-19

William Malik, VP of Infrastructure Technologies, Trend Micro
Mitchel Chang, VP of Global CSR and Education, Trend Micro
April 21, 2020
Trend Micro Initiative for Education

For more than 32 years, Trend Micro’s unwavering vision has been to make the world safe for exchanging digital information. This single-minded passion has inspired our innovations that keep up with the bad guys despite a changing IT landscape, riskier user behavior, and constantly evolving threats. Trend Micro Initiative for Education includes all of our community outreach efforts working to provide digital safety education and user awareness.

William Malik

Mitchel Chang
Social Distancing Impacts
Major Impacts of Social Distancing

• No Foot Traffic
  – Use different channels
  – Rely on different payment systems

• Employees Working from Home
  – Cope with changes in IT demand
  – Adjust management style for remote workers
Demand, Fulfillment, Payment

- On-line Ordering
  - Do you have an on-line channel? Etsy? Amazon?

- Third-party Fulfillment
  - Uber Eats? USPS?

- Ecommerce Payment Stream
  - Is your bank ready for Venmo? Square? PayPal?
Managing Remote Workers

• Supervisors Focus on Essentials
  – “Wandering around” doesn’t work
  – What really matters about team performance?

• IT Infrastructure Load
  – Network support (people) and capacity (load)
  – Home users on personal (family) machines
Protecting your small and medium business during COVID-19
Cybercrime Increased by 300%!

According to FBI on April 20, 2020, instances of cybercrime appear to have jumped by as much as 300 percent since the beginning of the coronavirus pandemic. The bureau’s Internet Crime Complain Center (IC3) is now receiving between 3K to 4K cybersecurity complaints per day, up from the average 1K per day before.

Opportunities for cyber criminals

- America’s daily activities increasingly moving online
- Newly remote workers unaware of basic security measures
- Companies struggling to keep externally-accessed systems secured
- Lack of social and work place interactions
- Ongoing uncertainties:
  - Supply chains (PPE and essential goods)
  - Online orders and payments
  - Medical help and COVID-19 testing
  - Fears and other factors….
Monthly spam email detections
(containing covid, covid-19, coronavirus, or ncov)

*Note that the detection numbers represent the coverage of our Smart Protection Network sensors, which have limited global distribution.

This data reflects findings from January 1 to March 31, 2020.
Instances that malicious COVID-19 related URLs were accessed

*Note that the detection numbers represent the coverage of our Smart Protection Network sensors, which have limited global distribution. This data reflects findings from January 1 to March 31, 2020.
The pandemic’s effects have reached the CYBERCRIMINAL UNDERGROUND

Popular Items Now Sold in the Underground

- Covid-themed phishing, malware, and exploits
- Toilet paper, N95 masks, ventilators, and other essential supplies
Phishing and scams using NETFLIX as lure

Activities Spotted

- Facebook login credentials are stolen
- Malicious links are posted via compromised accounts
SPAM: top method to deliver attacks on enterprises

94.9%

Top 2 Spam Samples

- Shipment Notification
- Coronavirus Ministry of Health Updates
COVID-19-Related Threats in Q1 2020

- 907K Total spam messages related to COVID-19
- 737 Detected malware related to COVID-19
- 48K Hits on malicious URLs related to COVID-19

- 220x Increase in spam from Feb to Mar 2020
- 260% Increase in malicious URL hits from Feb to Mar 2020

**United States**

Top location for spam and malware detections, and users accessing malicious URLs

*Detection numbers are based on the coverage of our Smart Protection Network, which has limited global distribution (collection period: January 1 to March 31, 2020).*
Business Email Compromise (BEC)

On April 6, 2020, Federal Bureau of Investigation (FBI) issued a warning anticipating a rise in BEC schemes related to the COVID-19 Pandemic.

“Fraudsters will take advantage of any opportunity to steal your money, personal information, or both. Right now, they are using the uncertainty surrounding the COVID-19 pandemic to further their efforts.”

According to FBI, there has been an increase in BEC frauds targeting municipalities purchasing personal protective equipment in the fight against COVID-19. Also, most of the recent BEC attacks were targeted at the financial institutions or banks.
Organized BEC Attackers

• A typical BEC attack would be launched by email. The emails are either spoofed or compromised by the attackers. For example, an attacker may pretend to be a vendor by requesting invoice or transaction payments.

• BEC attacker’s typical steps
  – Assessing to identify potential targets by using various searches in social media and on Internet sites
  – Creating a target list and send out phishing or spear phishing emails
  – Responding if the victim responds, engaging directly with some small exchanges to secure the fraud
  – Requesting financial transition by sending the money to a third party
  – Closing and repeating the same scam if possible
BEC Preventive Measures (recommendation)

• Avoid posting any personal identifiable information (PII) on Internet. For example, your birthday, Social Security or driver’s license number.

• Lessen the posting of any internal company or communities’ social activities to the public

• If you are not technically savvy, always leverage your IT person to check email headers if in doubt.

• Have a strong company policy and process

• Use cybersecurity tools
Protecting your business
cybersecurity hygiene fundamentals review
Best Practices – User Security (review)

- Passwords
- Email Safety
- Online Safety
- Remote and office
Best Practices – User Security

• Passwords
• Email Safety
• Online Safety
• Remote and office

- Cyber defense is no longer just behind your home or business network firewall
  ✓ Protecting your data is a must (versus just perimeter)
- Be cautious with public Wi-Fi
  ✓ Disable auto-join or auto-connect to popular public WiFi AP (i.e., airports, coffee ships, malls, restaurants)
  ✓ Understand how to use VPN and https
- Cloud service security and backup setup
  ✓ (One-Drive, Google Drive, Dropbox..etc.)
- Back-up strategy and process  <= important
  • On-premise and/or cloud
Best Practices – Device Security

- **Computers/Servers**
  - Centrally managed, business grade cybersecurity software coverage for cloud, web, email, server and network security
  - Ability to mitigate and recovery from a breach or cyber attack such as Ransomware
- **Mobile Devices**
- **Wi-Fi Routers**
- **Other Devices**
  - Isolate payment systems (home vs. work PC)
  - Restrict access to servers
  - Implement two-factor authentication
  - Update software/firmware regularly
Best Practices – Device Security

- Computers/Servers
  - Update operating system and apps regularly
  - Use built-in security features
  - Turn off any app permissions you do not use
  - Minimize location access
  - Disable Bluetooth when not required
  - Do not connect to unsecured Wi-Fi networks
  - Only download apps from trusted sources
  - Ignore and block unsolicited calls and messages. Do not return calls from unknown numbers
  - Use long, strong passwords
  - Minimize personal data in apps and websites
  - Consider using a vendor security product

- Mobile Devices
  - Turn off any app permissions you do not use
  - Minimize location access
  - Disable Bluetooth when not required
  - Do not connect to unsecured Wi-Fi networks
  - Only download apps from trusted sources
  - Ignore and block unsolicited calls and messages. Do not return calls from unknown numbers

- Wi-Fi Routers
  - Do not connect to unsecured Wi-Fi networks
  - Only download apps from trusted sources
  - Ignore and block unsolicited calls and messages. Do not return calls from unknown numbers
  - Use long, strong passwords
  - Minimize personal data in apps and websites
  - Consider using a vendor security product

- Other Devices
Additional Resources

SCORE
http://score.org

National Cyber Security Alliance (NCSA)
https://staysafeonline.org/
https://staysafeonline.org/cybersecure-business/

Cybercrime Support Network (CSN)
https://cybercrimesupport.org/

COVID-19 information from various Trend Micro Research and Education
www.trendmicro.com (coronavirus banner) or
https://resources.trendmicro.com/Coronavirusresources.html
Trend Micro endpoint solutions such as the **Smart Protection Suites** and **Worry-Free™ Business Security** detect and block the malware and the malicious domains it connects to.

**Trend Micro™ Email Security** thwarts spam and other email attacks. The protection it provides is constantly updated, ensuring that the system is safeguarded from both old and new attacks involving spam, BEC, and ransomware.

**Trend Micro Deep Discovery™ Email Inspector** detects and blocks ransomware spear phishing emails through advanced analysis techniques for known and unknown attacks.


A **multilayered protection** is also recommended for protecting all fronts and preventing users from accessing malicious domains that could deliver malware.
Thank You