Pirates without Borders: the Propagation of Cyberattacks through Firms' Supply Chains

- a discussion of the paper by **Matteo Crosignani, Marco Macchiavelli & André F. Silva**

Discussant: Monika Marcinkowska

UNIVERSITY OF LODZ

EBA EUROPEAN BANKING AUTHORITY | EBA BANKING STAKEHOLDER GROUP

2020 EBA POLICY RESEARCH WORKSHOP

"New technologies in the banking sector – impacts, risks and opportunities"

Paris, 12-13 November 2020

#1

Main findings of the research

pixabay.com

UNIVERSITY OF LODZ

Main findings

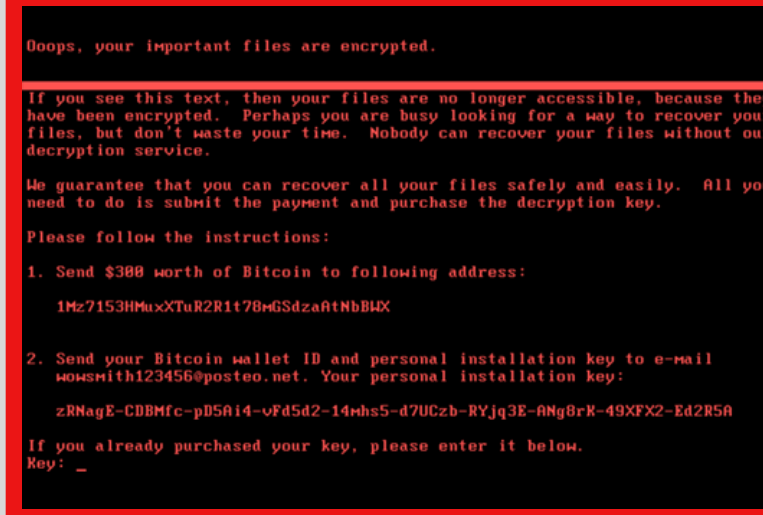
- The propagation effects through supply chains of the cyberattack
  - No significant upstream effects to the suppliers of the directly hit firms
  - Customers of directly hit firms saw reductions in revenues, profitability, and trade credit relative to similar firms
    - larger losses for customers with **fewer alternative suppliers** and suppliers producing **high-specicity inputs**
  - The shock led to persisting adjustments to the supply chain network
- The important role of banks in mitigating cyberattack impact
  - Affected firms used **internal liquidity buffers** and **increased borrowing**, mainly through bank credit lines (at higher rates due to increased risk), which helped affected customers to maintain investment and employment

https://pl.freepik.com

https://www.2-spyware.com/maersk-needed-10-days-to-recover-from-notpetya-attack-fully

Conclusions

- **Customers** of affected companies
  - *a signicant drop in customers' profitability relative to similar but unaffected firms,*
  - *the cyberattack caused a reduction in trade credit among affected customers that, in response, depleted their pre-existing liquidity buffers and increased borrowing*
  - *affected customers drew down their credit lines at higher interest rates after the shock due to increased risk*
  - *bank credit helped affected customers maintain their investment and employment*
  - *the downstream effects are driven by customers that have fewer alternatives for the directly hit supplier*
  - *affected customers formed new relationships with alternative suppliers after the shock, consistent with a wake up call effect of the cyberattack.*
- **Suppliers** of affected companies
  - *a negative effect on the profitability of affected suppliers, albeit small in magnitude and statistically insignificant.*

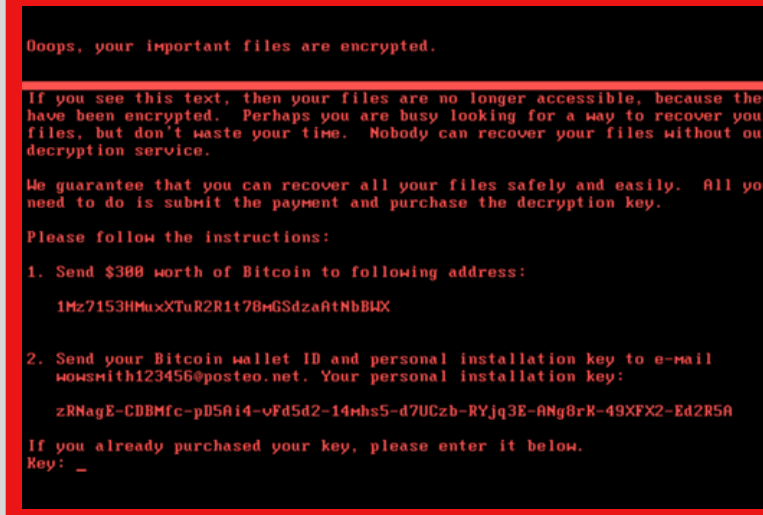


https://www.crowdstrike.com/blog/petrwrap-ransomware-technical-analysis-triple-threat-file-encryption-mft-encryption-credential-theft/

Conclusions

- The bottleneck occurred on the directly hit firms' ability to deliver their products to their **customers**
- Their **suppliers** could have still been able to deliver their products to the directly hit firms

- => results similar to other research:
  - **cyberattacks can create supply chain disruptions akin to those that originate from financial crises and natural disasters**



https://www.crowdstrike.com/blog/petrwrap-ransomware-technical-analysis-triple-threat-file-encryption-mft-encryption-credential-theft/

#2

General overview of the paper

pixabay.com

General overview

- **Subject**:
  - Consequences of cyberatack and their propagation through firms' supply chains
  - 2017 NotPetya attack
    - initial vector of infection - a tax reporting software in Ukraine
    - malware spread across different companies, including large global firms through their Ukrainian subsidiaries
- **Motivation for the research** (justification for the choice of the topic):
  - The destructive power of the cyberattacs
  - Huge and rising direct economic costs (3% of revenues on average in 2018)
  - **Unknown supply chain effects of cyberattacks**

General overview

- **Sample**
  - 10 public companies (different sectors) directly affected by NotPetya
  - Their customers and suppliers - a total of 201 customers and 314 suppliers indirectly affected by the cyberattack
    - Some excluded
    - financial data: intersection of 47,651 firm-year observations, corresponding to 10,640 firms from 2014 to 2018

		Full	Size Q1		Size Q2		Size Q3		Size Q4	
	Stat	Sample	Treated	Control	Treated	Control	Treated	Control	Treated	Control
No. Obs.	Tot	47651	356	14138	361	11831	358	12259	366	7982

    - 137,630 bank-firm-quarter observations from 2014:Q1 to 2018:Q4, covering 37 banks and 1,997 firms.
- **Method**
  - Difference-in-differences approach
    - Choice of the control group?

- **How many companies analysed eventually?** (would be useful to present a graph covering the selection process)
- **What was the share of analysed customers / suppliers in the 10 affected companies' revenues/costs?**

✓

?

General overview

- **Data sources**
  - Search of firms directly affected by NotPetya
    - web scraping SEC filings
    - a repository of international newspaper articles Dow Jones Factiva database
  - Global supply chain relationships data (customers and suppliers of those firms)
    - FactSet Revere (relationships between large - mostly publicly-listed - firms around the world)
  - Balance sheet and income statements information on firms from Orbis
  - Confidential credit register data for the US from the Federal Reserve's Y-14Q.

- **Time frame of the analysis**
  - June 2017 - cyberattack
  - SEC filings: 2017-2018
  - Time frame?
    - Data frequency?
  - 2014-2018
    - Quaterly data?
  - 2014Q1-2018Q4
- **Excellent use of different data sets**

General overview

- **Very important topic**
- **Very interesting analysis**
- **Impressive range of data**
- **Useful findings**
  - cyberattacks can create supply chain disruptions akin to those that originate from financial crises and natural disasters

https://pl.freepik.com

https://www.2-spyware.com/maersk-needed-10-days-to-recover-from-notpetya-attack-fully

#3

Potential limitations of the research
Questions and remarks

pixabay.com

UNIVERSITY OF LODZ

Sample

- 10 global firms directly affected
  - Excluded: firms from Ukraine and Russia and non-public firms (lack of data)
- A total of 201 customers and 314 suppliers indirectly affected by the cyberattack
- Supply chain relationships
  1) *[FactSet Revere]- the data set includes almost a million relationships between large (mostly publicly-listed) firms around the world*
  2) *We drop redundant relationships whose start and end dates fall within the period of a longer relationship between the same firm pair and combine multiple relationships between two firms into a continuous relationship if the time gap between two relationships is shorter than six months*
  3) *We merge Orbis with FactSet using the ISIN of each firm and disregard companies that are not present in both data sets to avoid selection bias due to the inclusion of smaller listed firms that appear in Orbis but that do not report supply chain relations.*
- *We find that the downstream disruption caused by the cyberattack is concentrated among customers that have fewer alternatives for the directly hit supplier. This holds both when considering how many other suppliers a customer has in the same industry of the directly hit supplier, and when focusing on suppliers of less substitutable goods and services - that is, suppliers providing high-specificity inputs.*

- **Questions**:
  - To what extend the sample (and its limitations) might influence the outcomes of the study?
    - Large firms relations only
      - What portion of relationships are covered?
      - Is there a possibility that smaller firms' (not included in the analysis) reactions were different?
      - Non-diversified suppliers/customers?
      - If so, this would mean that they HAD no option but to change their suppliers
      - => would be useful to check concentration of suppliers/customers and group the sub-samples in the analysis

Method

- Difference-in-differences approach

- *we use a difference-in-diferences approach, comparing the change in behavior of firms indirectly affected by the shock through their supply chain with that of unaffected firms operating in the same industry, country, and size quartile in the same year*

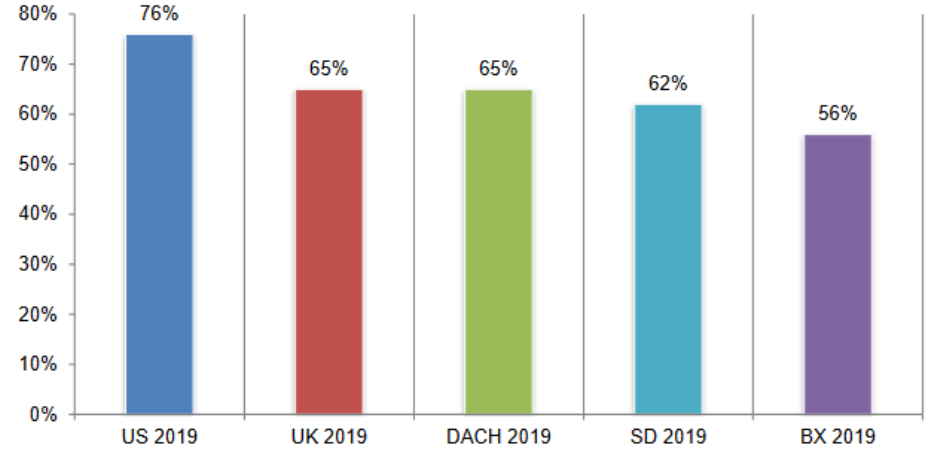
- **Questions**:
  - Selection of control group?
    - Sure they were unaffected by cyberattacs?
  - Potential other analysis: differences not only between groups of companies, but in periods covered (provided continued relationships)

Sample

- Sample and control group

- **Questions and remarks**:
  - How was the control group chosen?
  - There is a risk that the both groups – sample and control - consist of companies directly and/or indirectly affected by cyberattacks

Figure 21. Has your organization experienced a cyberattack in the past 12 months?



Ponemon INSTITUTE

Exclusive Research Report
2019 Global State of Cybersecurity in Small and Medium-Sized Businesses

Data

- Bank credit to firms (Federal Reserve's Y-14Q)
  - Data for the large banks in the US
    - **credit exposures** exceeding $1 million for banks with more than $50 billion in assets (75% of all commercial and industrial lending volume)
    - information on each bank's internal assessment of the **probability of default** of a given firm (a model-based metric that captures the bank's hard information about a given borrower and that predicts loan delinquency)

- **Questions**:
  - To what extend the data sources (and its limitations) this might influence the outcomes of the study?
    - US banks only
      - Not all of the analysed firms have loans in the US banks (or not only US banks)
    - Only the data for big banks and big loans
      - Given the size of the analysed firms, is there a possibility that they have loans in smaller banks or smaller loans in analysed banks?
    - => If so, this would mean that that not all data is captured

#4

Some questions and suggestions
Further research

pixabay.com

UNIVERSITY OF LODZ

Findings

- *The shock led to persisting adjustments to the supply chain network*

Affected customers formed new relationships with alternative suppliers after the shock, consistent with a wake up call effect of the cyberattack

Customers are likely to take immediate steps to form new trading relations with alternative suppliers and later on terminate those with the suppliers that caused the disruption

Estimates indicate that affected customers are more likely than similar firms in the control group to terminate suppliers in the same industry as the directly hit one.

- **Questions**:
  - Whas it a **permanent** change of a supplier?
    - (suggested longer period of analysis)
  - If relations with suppliers are terminated in the industry, is it actually the effect of an attack?
    - in case of avoiding the affected company, customers should swich the supplier and not terminate suppliers in the same industry - vide the second sentence

Findings

- *Affected customers used their **internal liquidity buffers** and **increased borrowing**, mainly through bank credit lines at higher rates due to increased risk, helped affected customers to maintain investment and employment.*

Were there any regulatities which firms used which source / to what extend?

Other questions / suggestions

- „Pirates without borders"
  - International contagion of direct consequences of the attack
  - What about indirect consequences – any differences/similarities for domestic/international supply chains?
- Any differences/regularities among different industries?

#5
Policy implications

UNIVERSITY OF LODZ

pixabay.com

Policy implications

- Better cybersecurity
  - more compartmentalization of the network infrastructure,
  - more scrutiny on the cybersecurity of third-party suppliers,
  - one backup facility that is offine at any time;
- Firms need to improve their risk management and contingency planning
  - being able to continuing activities in the event that anyone of their suppliers is unable to provide goods and services
  - the resilience of a supply chain rests on having multiple options for each intermediate good or service, so that no single supplier is irreplaceable
- The intelligence community should establish credible deterrence for cyber-aggressions of the magnitude of NotPetya, so that state-sponsored hackers at least have an incentive to put in place controls to make sure that the attack does not spread beyond its intended reach

✓

✓

???

pixabay.com

Conclusions

- The general conclusion supportes the results similar to other research:
  - **cyberattacks can create supply chain disruptions akin to those that originate from financial crises and natural disasters**
  - => important for the analysis (and management) of supply chain disruptions of any kind

pixabay.com

Thank you for your attention!

UNIVERSITY OF LODZ

monika.marcinkowska@uni.lodz.pl