NotPetya
June 27, 2017

Group 4
Shannon Smith
Michael Kaupert

(Reference 12)

1 SUMMARY

THE WORST CYBERATTACK IN HISTORY

(References 2, 3 & 7)

The NotPetya cyberattack, which struck on the eve of Ukraine's Constitution Day, was intended for the Ukrainian government and businesses inside the country. Of the industries impacted, 80% were in the financial, energy, and manufacturing sectors alone. The attack has cost an estimated 10 billion dollars in economic damages worldwide, making it the most expensive attack to date.

The damage spread within hours, distributed through a hacked update server for Linkos Group's business software M.E. Doc in Ukraine, and was disguised to look like ransomware, but the intent was destruction. Exploits such as Mimikatz, EternalBlue, and EternalRomance, rendered computers useless to users and spread via LAN using administrative credentials obtained through the malware.

Russian operatives who call themselves "Sandworm Team" are to blame for the attacks and are part of the Russian GRU. The purpose was to destabilize the Ukraine economy, but damages were much more far-reaching.

2 WHO

NATION-STATE ATTRIBUTION

(References 1, 11 & 14)

"Sandworm Team", a destructive threat group that is part of Russia's General Staff Main Intelligence Directorate (GRU) Main Center for Special Technologies (GTsST) military unit 74455, has been held responsible for NotPetya

- Six members indicted in the U.S. for NotPetya
- Also responsible for malware attacks KillDisk, Industroyer, and Olympic Destroyer
- Allegedly contributed to a phishing attack on the Democratic National Committee and other electoral interference campaigns during the 2016 U.S. presidential election
- Associated groups with Sandworm Team are "ELECTRUM," "BlackEnergy (Group)," "Quedagh," "Voodoo Bear," and "Iron Viking"

Some of the attacks conducted by GRU Unit 74455 were aided by GRU Unit 26165, also referred to as APT28

MEMBERS OF GRU RESPONSIBLE

(References 13 & 14)

YURIY SERGEYEVICH ANDRIENKO
(Юрий Сергеевич Андриенко)

PAVEL VALERYEVICH FROLOV
(Павел Валерьевич Фролов)

YURIY SERGEYEVICH ANDRIENKO
(Юрий Сергеевич Андриенко)

SERGEY VLADIMIROVICH DETISTOV
(Сергей Владимирович Детистов)

ANATOLIY SERGEYEVICH KOVALEV
(Анатолий Сергеевич Ковалев)

ARTEM VALERYEVICH OCHICHENKO
(Артем Валерьевич Очиченко)

TIMELINE OF SANDWORM ACTIVITIES

(Reference 13)

- **Dec 2015 - Dec 2016** — Ukrainian Government & Critical Infrastructure
- **April & May 2017** — French Elections
- **June 27 2017** — Worldwide Businesses & Critical Infrastructure **(NotPetya)**
- **Dec 2017 - Feb 2018** — PyeongChang Winter Olympics Hosts, Participants, Partners, & Attendees
- **Dec 2017 - Feb 2018** — PyeongChang Winter Olympics IT Systems (Olympic Destroyer)
- **April 2018** — Novichok Poisoning Investigations
- **2018 - 2019** — Georgian Companies & Government Entities

WHO WAS AFFECTED

(References 2, 4, 5, 10 & 16)

COMPANIES

- Antonov
- Rosneft
- Heritage Valley Health System
- DLA Piper
- Merck & Co.
- Saint Gobain
- TNT
- Mondelez Int'l
- A.P. Moller-Maersk
- WPP plc
- Reckitt Benckiser
- Beiersdorf
- DHL
- Cadbury

COUNTRIES

- Belgium
- Brazil
- Denmark
- France
- Germany
- India
- Russia
- Spain
- The Netherlands
- Ukraine
- United Kingdom
- United States
- Australia

INDUSTRIES

- Airports
- Banks
- Electricity grids
- Factories (mining and steel)
- Government
- Harbor terminals
- Hospitals
- Insurance companies
- Metro transportation
- Military
- Pharmaceutical
- Russian steel

$10,000,000,000

In economic damages worldwide

64 countries

Most businesses impacted were in the Ukraine

30%

Financial

25%

Energy

25%

Manufacturing

(References 9 & 16)

3 WHY

PURPOSE OF THE ATTACK

(References 5 & 10)

The NotPetya attack, which commenced the day before Ukrainian Constitution Day of June 28th, is one of many cyber attacks by Russia for purposes of destabilizing the country:

- Negatively influence public trust in the Ukrainian government, state, and industry sectors
- Dissuade businesses from operating and investing in Ukraine, which in turn would destabilize the economy
- Hopes of establishing new leadership in Ukraine, which would be more favorable to Russia
- To prepare for military action similar to the annexation of Crimea in 2014 (attacks that we are seeing since February 2022)

"This was a piece of malware designed to send a political message: If you do business in Ukraine, bad things are going to happen to you."

(Reference 3)

4 HOW

TECHNIQUES OF THE ATTACK

(References 2 & 11)

Sandworm hacked the M. E. Doc Accounting Software update servers

- The malicious update is pushed to the clients
- Once the update is installed, encryption of the machine starts

The malicious update used password harvesting (open-source Mimikatz) to gather administrative credentials for the local network

The harvested passwords are then passed to tools such as PSExec and WMIC

- These tools are used to infect other machines on the local network
- Two leaked exploits are used: ETERNALBLUE and ETERNALROMANCE to spread via the Local Area Network (LAN)

5 SO WHAT?

IMPACT TO THE VICTIMS

(References 8, 9 & 11)

- Primary targets were the government of Ukraine and corporations within Ukraine.

- 10 billion dollars in total economic damages and losses worldwide
  - Merck - $135 million in lost sales and $240 million in shutdowns
  - FedEx - loss of $300 million
  - Maersk - loss of $300 million

- Hard Costs
  - Damage to data - if not backed up, it was lost.
  - Damage to hardware - not physical, needed reimaging.

- Soft Costs
  - Damage to the reputation of the government and national corporations
  - Man-hours required to restore and bring systems back online
  - Reduced productivity until all damage was repaired

BROADER SIGNIFICANCE OF THIS EVENT

(References 11, 15 & 16)

- Affected companies fighting with insurance carriers over insurance reimbursement because the attack was deemed “warlike” so it could be excluded from coverage
- Terms like “cyber terrorism” and “cyberwar” are still being debated amongst academia, lawmakers, and insurance companies
- The importance of backing up data to recover quicker from an attack such as NotPetya
- Testing updates from third-party vendors before installing them on production equipment for consequential behavior

6 REFERENCES

1. Brewster, Thomas. "NotPetya Ransomware Hackers 'Took Down Ukraine Power Grid.'" *Forbes*, https://www.forbes.com/sites/thomasbrewster/2017/07/03/russia-suspect-in-ransomware-attacks-says-ukraine/. Accessed 20 Mar. 2022.
2. "Everything you need to know about the Petya, er, NotPetya nasty trashing PCs worldwide". 28 Jun 2017, https://www.theregister.com/2017/06/28/petya_notpetya_ransomware/.
3. Greenberg, Andy. "The Untold Story of NotPetya, the Most Devastating Cyberattack in History." *Wired*, 22 Aug. 2018, https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/.
4. "Industrial Cybersecurity Pulse - Throwback Attack: How NotPetya Accidentally Took down Global Shipping Giant Maersk." Industrial Cybersecurity Pulse, 30 Sept. 2021, https://www.industrialcybersecuritypulse.com/throwback-attack-how-notpetya-accidentally-took-down-global-shipping-giant-maersk/.
5. Janofsky, Kim S. Nash, Sara Castellanos and Adam. "One Year After NotPetya Cyberattack, Firms Wrestle With Recovery Costs." Wall Street Journal, 27 June 2018. www.wsj.com, https://www.wsj.com/articles/one-year-after-notpetya-companies-still-wrestle-with-financial-impacts-1530095906.
6. "NotPetya Ransomware Attack [Technical Analysis]." *Crowdstrike.Com*, 29 June 2017, https://www.crowdstrike.com/blog/petrwrap-ransomware-technical-analysis-triple-threat-file-encryption-mft-encryption-credential-theft/.
7. *NotPetya, Software S0368 | MITRE ATT&CK®*. https://attack.mitre.org/software/S0368/. Accessed 20 Mar. 2022.
8. "NotPetya: What We Know So Far." *Gigamon Blog*, 28 June 2017, https://blog.gigamon.com/2017/06/28/notpetya-what-we-know-so-far/.

9. NotPetya: World's First $10 Billion Malware. 28 Oct. 2017, https://www.apextechservices.com/topics/articles/435235-notpetya-worlds-first-10-billion-malware.htm#.

10. "Past Cyber Operations Against Ukraine and What May Be Next." *Crowdstrike.Com*, 28 Jan. 2022, https://www.crowdstrike.com/blog/lessons-from-past-cyber-operations-against-ukraine/.

11. *Petya (NotPetya, Petrwrap)*. 28 June 2017, https://www.anomali.com/blog/petya-notpetya-petrwrap.

12. "Petya Ransomware Outbreak Originated in Ukraine via Tainted Accounting Software." *BleepingComputer*, 27 June 2017, https://www.bleepingcomputer.com/news/security/petya-ransomware-outbreak-originated-in-ukraine-via-tainted-accounting-software/.

13. "Six Russian GRU Agents Indicted in Connection With NotPetya Attack." The Maritime Executive, 19 Oct. 2020, https://www.maritime-executive.com/article/six-russian-gru-agents-indicted-in-connection-with-notpetya-attack.

14. *Six Russian GRU Officers Charged in Connection with Worldwide Deployment of Destructive Malware and Other Disruptive Actions in Cyberspace*. 19 Oct. 2020, https://www.justice.gov/opa/pr/six-russian-gru-officers-charged-connection-worldwide-deployment-destructive-malware-and.

15. "Was It an Act of War? That's Merck Cyber Attack's $1.3 Billion Insurance Question." *Insurance Journal*, 3 Dec. 2019, https://www.insurancejournal.com/news/national/2019/12/03/550039.htm.

16. Whitfield, Paul. "Cyber Attack Likely Cost Saint-Gobain 1% of First Half Sales." *TheStreet*, 13 Mar. 2017, https://www.thestreet.com/investing/cyber-attack-likely-cost-saint-gobain-1-of-first-half-sales-14226649.