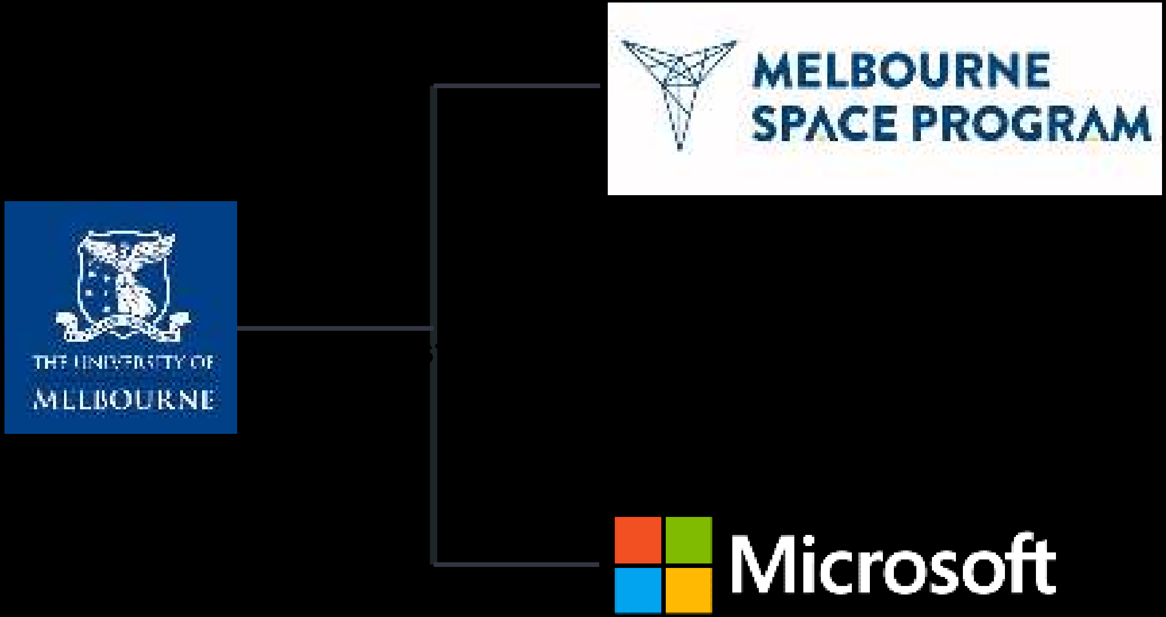
NotPetya

One of The Most Devastating Cyberattack in History

Kaif Ahsan


THE UNIVERSITY OF MELBOURNE
MELBOURNE SPACE PROGRAM
Microsoft

What’s the worst thing that can happen from a cyberattack?

victim of the PETYA RANSOMWAR

ks of your computer ha te

algorithm. There is to re

n purchase this key he da

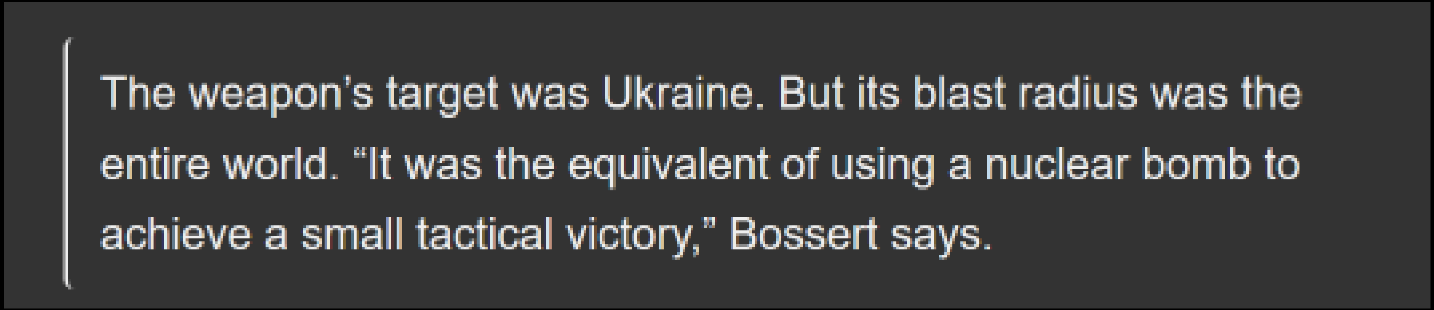
e your key and restor

the Tor Browser at "https:

gle for "access oni

Damage on Ukraine

- The radiation monitoring system at Ukraine's Chernobyl Nuclear Power Plant went offline
- Several Ukrainian ministries, banks, metro systems and state-owned enterprises
- 1,500 legal entities and individuals



> The weapon's target was Ukraine. But its blast radius was the entire world. “It was the equivalent of using a nuclear bomb to achieve a small tactical victory,” Bossert says.

Notable Companies Affected by NotPetya

○ Maersk

○ FedEx

○ Merck

○ Mondelēz (Cadbury & Nabisco)

And almost 300 More!

$10,000,000,000,000

National State Level Sophistication

An Autopsy Report

1. Disguised as a ransomware worm. Similarity to Petya

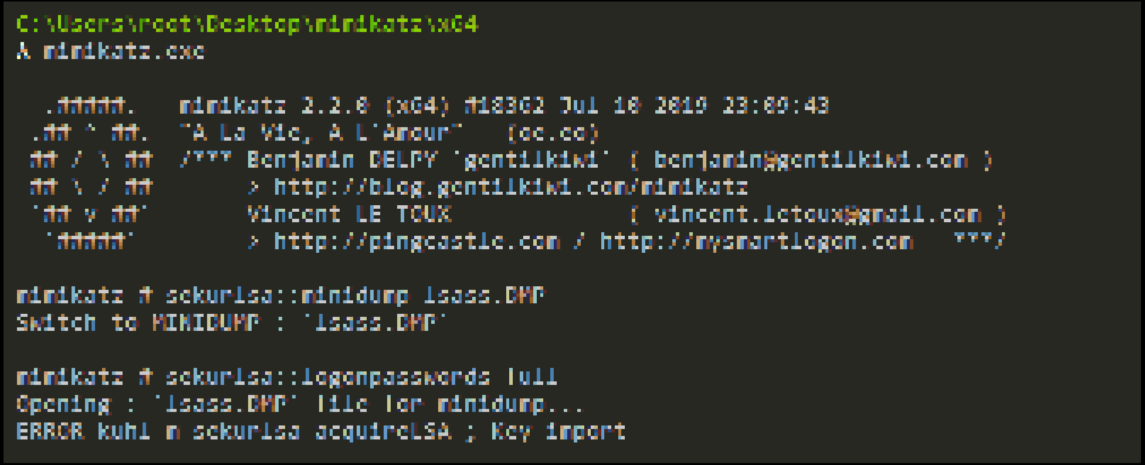
2. Combined with two very powerful exploits

3. Linkos group’s M.E.Doc was used to spread the malware

Mimikatz

Tool to extract plaintexts passwords, hash, PIN code and Kerberos tickets from memory.

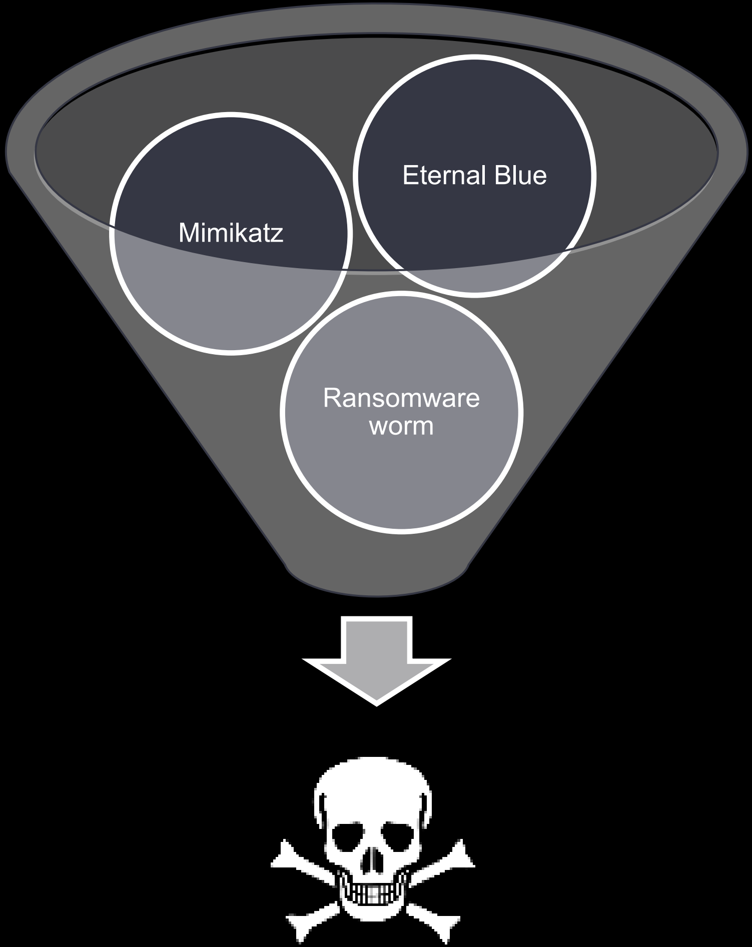
- Takes advantage of Lsass.exe
- Pass hashes, tickets, Kerberos golden and silver tickets



```
C:\Users\root\Desktop\mimikatz\x64
λ mimikatz.exe

  .#####.   mimikatz 2.2.0 (x64) #18362 Jul 10 2019 23:09:43
 .## ^ ##.  "A La Vie, A L'Amour"   (oe.eo)
 ## / \ ##  /*** Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
 ## \ / ##       > http://blog.gentilkiwi.com/mimikatz
 '## v ##'       Vincent LE TOUX             ( vincent.letoux@gmail.com )
  '#####'        > http://pingcastle.com / http://mysmartlogon.com   ***/

mimikatz # sekurlsa::minidump lsass.DMP
Switch to MINIDUMP : 'lsass.DMP'

mimikatz # sekurlsa::logonpasswords full
Opening : 'lsass.DMP' file for minidump...
ERROR kuhl_m_sekurlsa_acquireLSA ; Key import
```

Eternal Blue

- Developed by NSA, leaked by Shadow Brokers
- Used in the WannaCry ransomware attack
- Exploits a vulnerability in Microsoft's implementation of the Server Message Block (SMB) protocol.



Mimikatz

Eternal Blue

Ransomware worm

Who? Why?

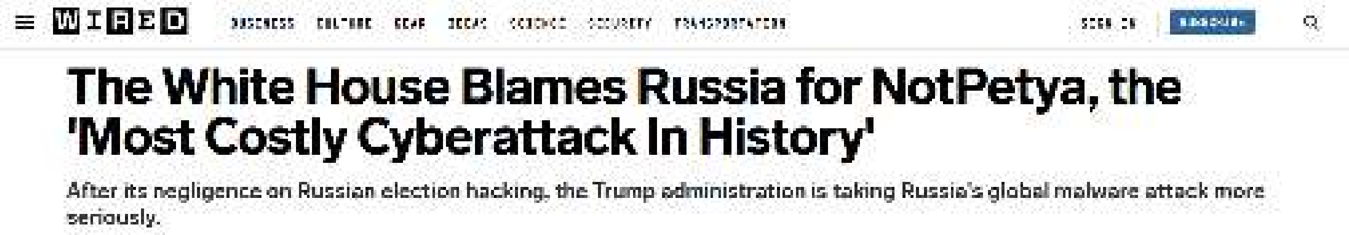
Rogue Hacker Group or National State Agent?

- Researchers starting pulling the code apart

- Slovakian Security firm ESET collect forensic evidence which tie it Sandworm

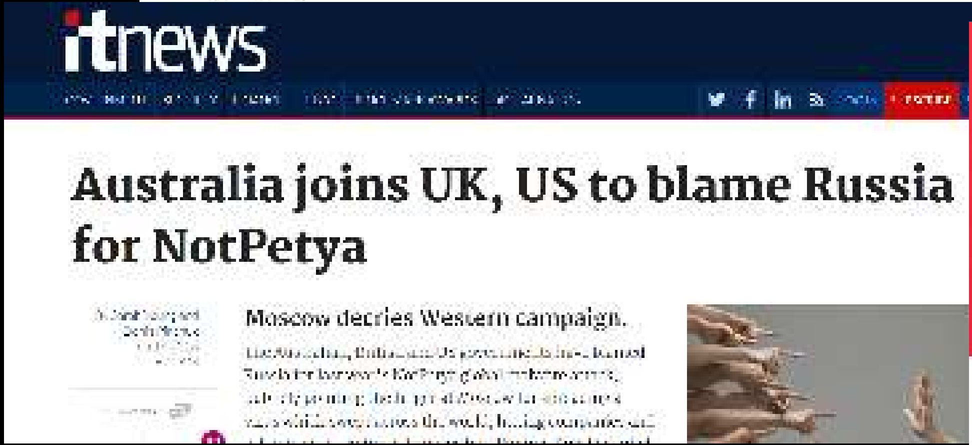
- Malware attack on the Ukrainian power grid as well as a mining company and a large railway operator in December 2015

Changing the cyberwar landscape



The White House Blames Russia for NotPetya, the 'Most Costly Cyberattack In History'

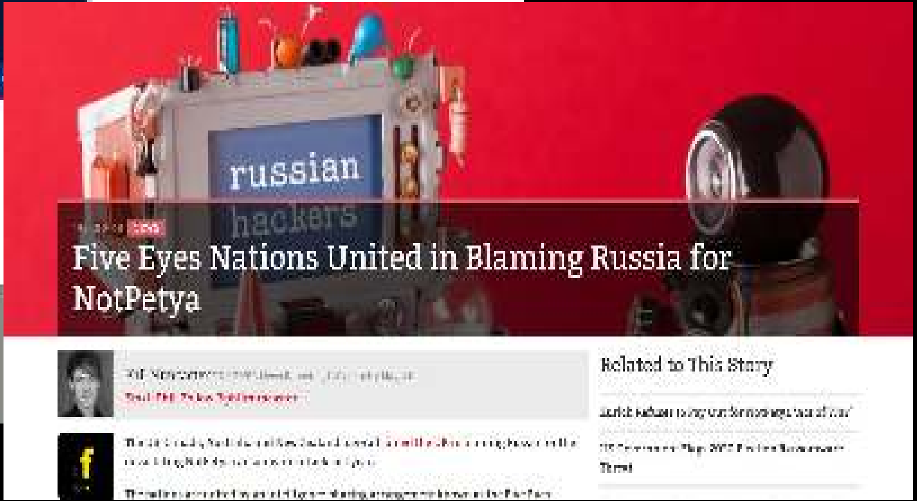
After its negligence on Russian election hacking, the Trump administration is taking Russia's global malware attack more seriously.



Australia joins UK, US to blame Russia for NotPetya

Moscow decries Western campaign.

[illegible]



Five Eyes Nations United in Blaming Russia for NotPetya

Related to This Story

[illegible]

Food For Thought

- Why did Russia leak Eternal Blue in the first place?
- Why no visible action was taken against Russia?

Thank You!