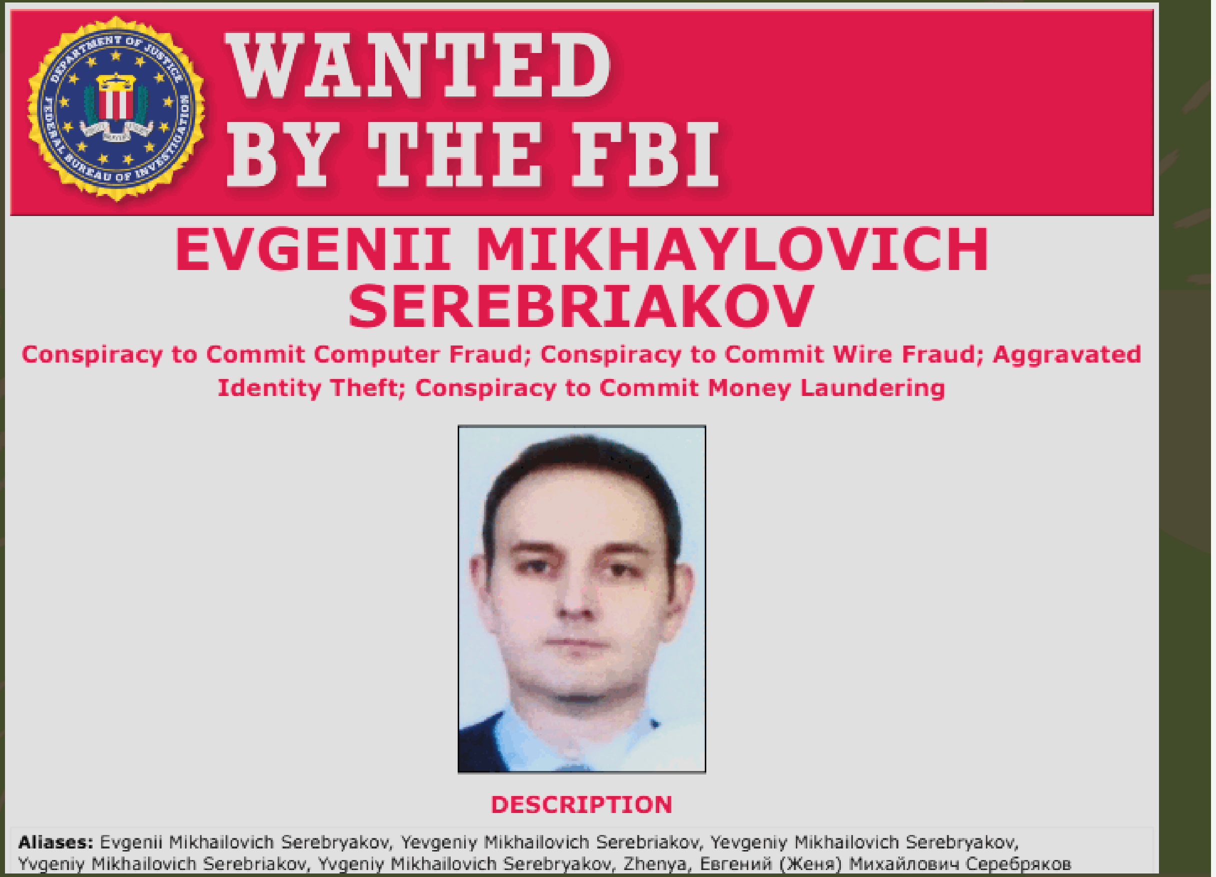
Sandworm

An Overview of the Advanced Persistent Threat (APT) group “Sandworm”

Jordan Patterson 2024



WANTED BY THE FBI

EVGENII MIKHAYLOVICH SEREBRIAKOV

Conspiracy to Commit Computer Fraud; Conspiracy to Commit Wire Fraud; Aggravated Identity Theft; Conspiracy to Commit Money Laundering

DESCRIPTION

Aliases: Evgenii Mikhailovich Serebryakov, Yevgeniy Mikhailovich Serebriakov, Yevgeniy Mikhailovich Serebryakov, Yvgeniy Mikhailovich Serebriakov, Yvgeniy Mikhailovich Serebryakov, Zhenya, Евгений (Женя) Михайлович Серебряков

Suspected Attribution

- The Sandworm Hacker group is led by Evengii Serebriakov
- Other members are officers of the Russian Main Intelligence Directorate (GRU) and include:
  - Yuriy Sergeyevich Andrienko
  - Sergey Vladimirovich Detistov
  - Pavel Valeryevich Frolov
  - Anatoliy Sergeyevich Kovalev
  - Artem Valeryevich Ochichenko
  - Petr Nikolayevich Pliskin

Prosecution

- In 2020, The US Department of Justice charged 6 members of Sandworm with crimes related to their Cybercrimes. It has been estimated that Sandworms cyberattacks have caused over 1 Billion dollars in losses.
- The crimes were:
  - conspiracy to conduct computer fraud and abuse
  - conspiracy to commit wire fraud
  - wire fraud
  - damaging protected computers
  - aggravated identity theft

Sponsors

- Sandworm is completely state sponsored and part of the Russian Military.
- Sandworm is also known as Unit 74455 of the Russian Cybermilitary unit of the GRU. The GRU is in charge of Russian military intelligence.
- The group not only publically goes by the name Sandworm but may also be seen going by the names Telebots, Iron Viking, and Voodoo Bear.

Target Sectors

- Sandworm often targets large sectors such as the industrial sector, politics, and international sports.
- Notable targets in these sectors include the Ukrainian power grid/companies in 2015/2016, the 2017 French presidential election, and the 2018 Winter Olympic games.

Motivation

- Sandworms motivations are political in nature, mainly falling into the categories of Cyber Espionage, Cyber Warfare, and Sabotage.

- This APT groups motivations serve the strategic interests of the Russian Government and Military.

Attack Vectors

- Backdoors in Operational Technology systems; Internet connected inductrial systems
- Zero-Day exploits
- Spearphishing
- Malware; BlackEnergy, NotPetya
- Email Software exploitation; Exim Mail Transfer Agent (MTA)

Associated Tools and Malware in Each Phase

Initial Compromise:

- Spearphishing
- Zero-Day exploits
- BlackEnergy Malware: An HTTP-based toolkit that generated bots to execute distributed denial of service attacks. BlackEnergy is also capable of data exfiltration.
- Neo-REGEORG: A web shell generation tool designed to establish a SOCKS proxy on the compromised system.
- Exim Mail Server Exploitation: Sandworm has been exploiting vulnerable Exim mail servers since at least August 2019, using the hacked servers as an initial infection point on target systems.
- MEDoc Software Exploitation: A common piece of Ukrainian accounting software, to initially install its data-destroying, self-spreading code on its victims' machines.

Associated Tools and Malware in Each Phase

Lateral Movement:

- GOGETTER: A Golang-based tunneler, facilitated lateral movement.
- Living off the Land (LotL) Techniques: Sandworm used Operational technology level LotL techniques to disrupt the victim's machinery.
- Poemgate and Poseidon Backdoors: These backdoors capture the credentials of admins who attempt to authenticate in the compromised endpoint, providing the attackers with access to additional accounts they can use for lateral movement or deeper network infiltration.

Associated Tools and Malware in Each Phase

Data Exfiltration:

- Data Encryption: Sandworm has used Prestige ransomware to encrypt data at targeted organizations in transportation and related logistics industries in Ukraine and Poland.
- Data from Local System: Sandworm has exfiltrated internal documents, files, and other data from compromised hosts. Often using their BlackEnergy Malware.

Typical Tactics, Techniques, and Procedures

- Spearphishing to gain access
- Use of malware
- Exploitation of software vulnerabilities
- Living off the Land techniques to exploit industrial machinery
- Command and Control (C2) servers to manage their attacks
- Data encryption with Ransomware
- Disruption of critical infrastructure

Best-Known Compromise

- Sandworms best known compromise is the 2015 and 206 cyberattacks on the Ukranian Power Grid.
- These attacks caused widespread blackouts across the country of Ukraine.
- These attacks were the first successful cyberattacks against a power grid.

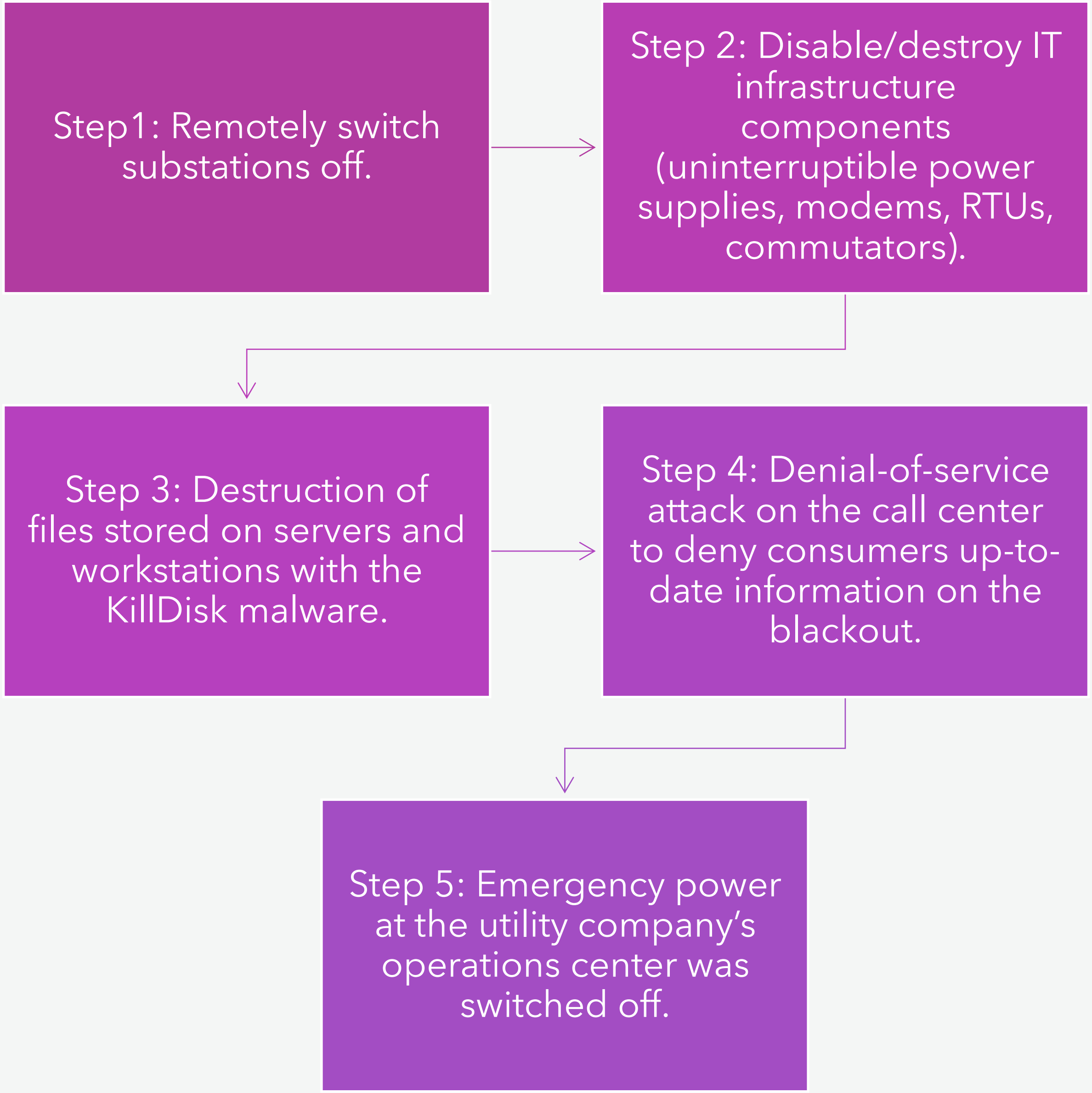
Overview of the Process of a Successful Attack

Initial Compromise: The initial compromise was achieved through spear-phishing emails with BlackEnergy malware. The hackers remotely compromised the information systems of three energy distribution companies in Ukraine.

Lateral Movement: After the initial compromise, the attackers had access to the SCADA system for up to three months. They leveraged an optical disc (ISO) image named "a.iso" to execute a native MicroSCADA binary in a likely attempt to execute malicious control commands to switch off substations.

Data Exfiltration: The BlackEnergy malware used in the attack has evolved into a sophisticated tool for data exfiltration. It's possible that the attackers could have used it to unauthorizedly transfer data from the compromised systems.

Execution of a Successful Attack



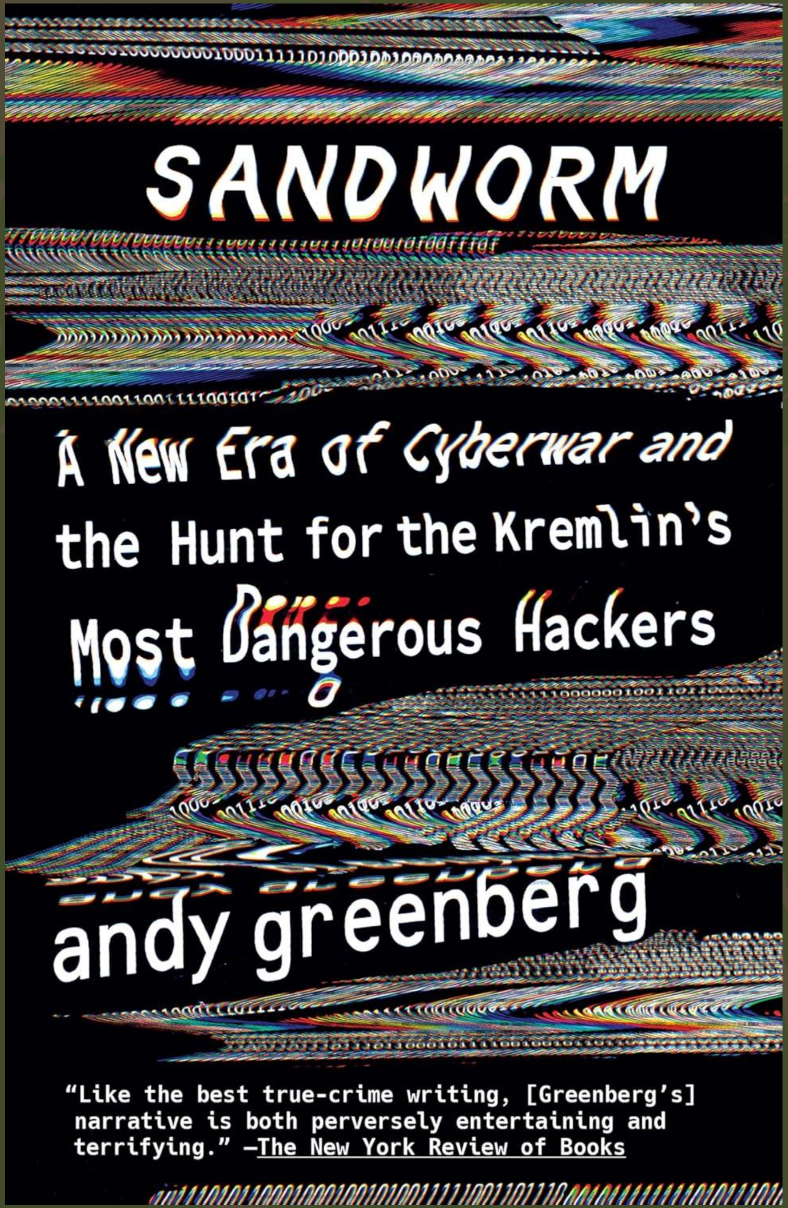
Step1: Remotely switch substations off.

Step 2: Disable/destroy IT infrastructure components (uninterruptible power supplies, modems, RTUs, commutators).

Step 3: Destruction of files stored on servers and workstations with the KillDisk malware.

Step 4: Denial-of-service attack on the call center to deny consumers up-to-date information on the blackout.

Step 5: Emergency power at the utility company’s operations center was switched off.


SANDWORM
A New Era of Cyberwar and the Hunt for the Kremlin's Most Dangerous Hackers
andy greenberg
"Like the best true-crime writing, [Greenberg's] narrative is both perversely entertaining and terrifying." —The New York Review of Books

Investigation and available material

- Sandworm has been extensively investigated by intelligence agencies and security researchers.
- A book was written and published about them in 2020 by Andy Greenberg called "Sandworm: A New Era of Cyberwar and the Hunt for the Kremlins Most Dangerous Hackers".
- This is one of the first books that was suggested to me at the beginning of my cybersecurity journey several years ago and I recommend it to anybody interested in Cybersecurity.

Sources

- https://attack.mitre.org/groups/G0034/
- https://www.amazon.ca/Sandworm-Cyberwar-Kremlins-Dangerous-Hackers/dp/0525564632/ref=tmm_pap_swatch_0?_encoding=UTF8&qid=&sr=
- https://www.justice.gov/opa/pr/six-russian-gru-officers-charged-connection-worldwide-deployment-destructive-malware-and
- https://dbpedia.org/page/Sandworm_(hacker_group)
- https://en.wikipedia.org/wiki/Sandworm_(hacker_group)
- https://en.wikipedia.org/wiki/BlackEnergy
- https://www.fbi.gov/wanted/cyber/evgenii-mikhaylovich-serebriakov/evgenii-mikhaylovich-serebriakov-8-5x11.pdf/view
- https://medium.com/readme/sandworms-kingpin-a-cisa-ransomware-pilot-and-pandemic-scams-25572eaf6b68