Kill Disk (and its use in hacks on the Ukranian Power Grid)

By: Mohamed Morsi, Rami Abu-Nassar and Ali Shahrami

Panic at the station!

The operator noticed that the cursor skittered across the screen.

Ghosts in the machine clicked open one breaker after the other.

Who was behind it all?

What did they do?

The attackers used multiple approaches to impac communication tools & facility infrastructure.

Seven 110kV and 2335 kV substations were disconnected for three hours.

Attack resulted in several outages that caused 225,000 customers to lose power.

Spear Phishing

The attacks began last spring with a spear phishing campaign that targeted IT staff and system administrators.

The attackers used spear phishing to plant BlackEnergy3 malware.

Used to gain access to the business networks of the oblenergos.

Telephone DoS

Used to prolong the outage.

Attackers used telephone systems to flood the call centers & deny access to them.

How was it different from other attacks?

- Nothing was inherently specific to the Ukrainian Infrastructure with the Killdisk Attack.

- StuxNet seeks out the Windows computers running specific configurations of the Siemens PLC software.

- Stuxnet intention was to cripple Iran’s suspected nuclear weapons program. Killdisk disrupted the Ukranian power plant.

Kill Disk – Technical Aspects

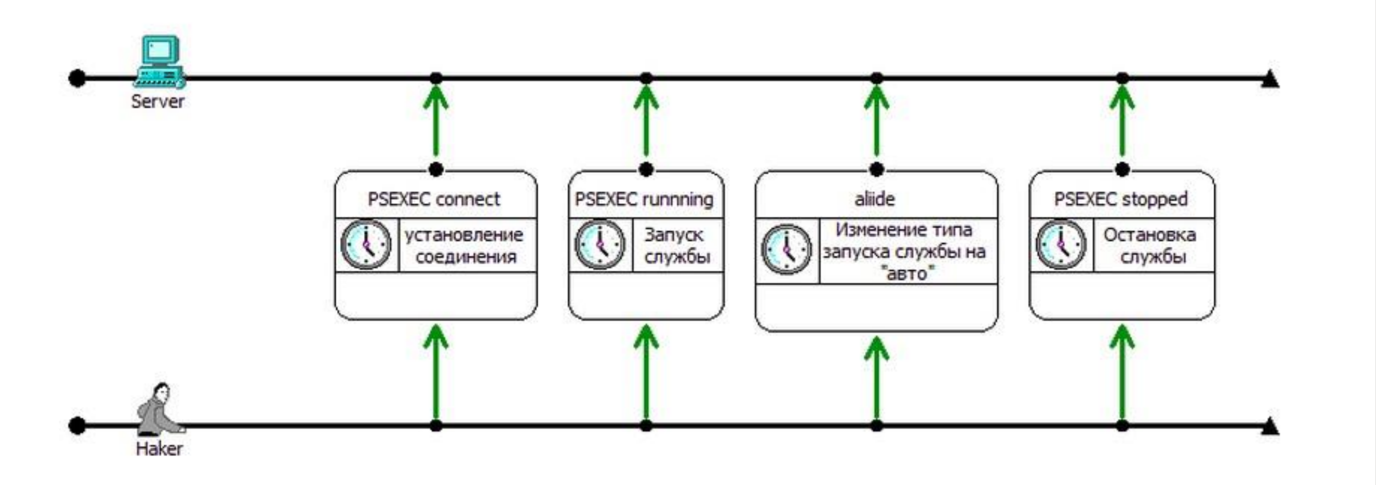
Russian Meme

- Publicly known as “Kill Disk”
- Actual name “ololo.exe” – reference to a Russian meme

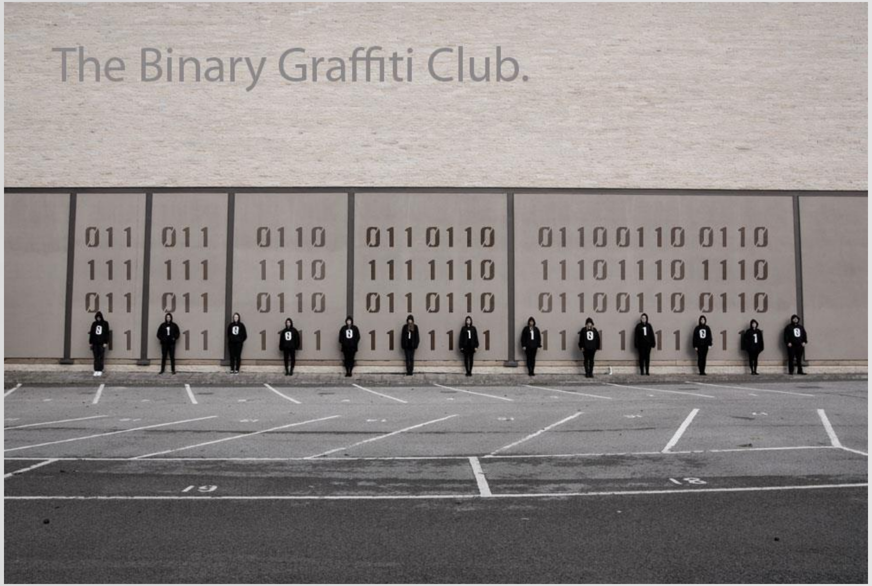
Brief Overview

- KillDisk is a destructive component that is used by these attackers as the final stage of the attack.
- Designed to run with high privileges.
- Deletes important system files making a computer un-bootable.

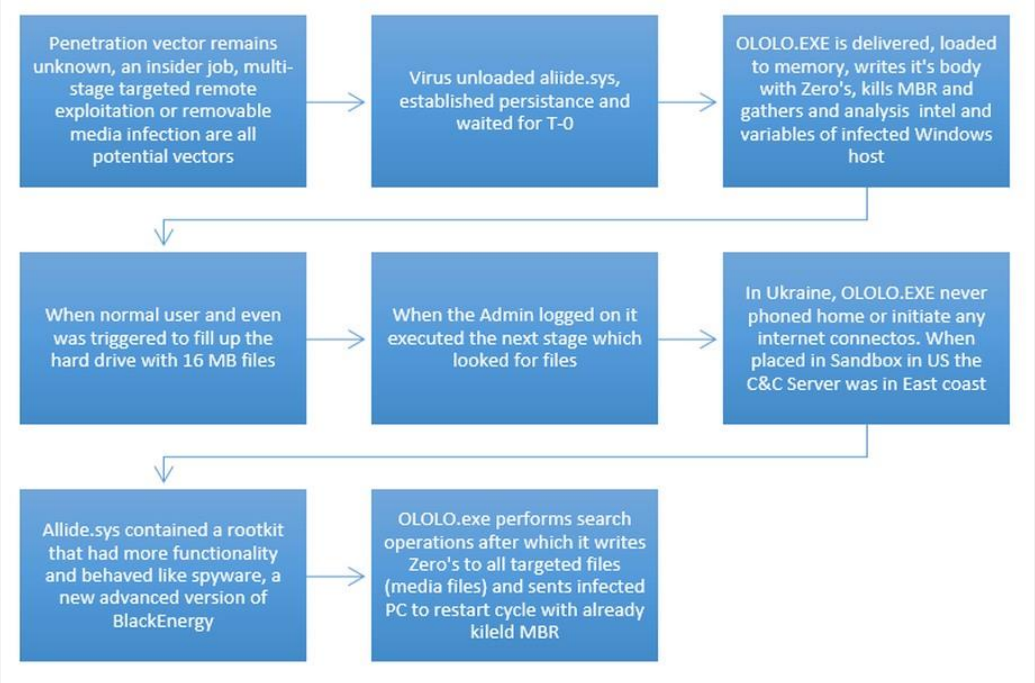
Payload - Specifics



From Payload to Art



Attack Stages map



Penetration vector remains unknown, an insider job, multi-stage targeted remote exploitation or removable media infection are all potential vectors

Virus unloaded aliide.sys, established persistance and waited for T-0

OLOLO.EXE is delivered, loaded to memory, writes it's body with Zero's, kills MBR and gathers and analysis intel and variables of infected Windows host

When normal user and even was triggered to fill up the hard drive with 16 MB files

When the Admin logged on it executed the next stage which looked for files

In Ukraine, OLOLO.EXE never phoned home or initiate any internet connectos. When placed in Sandbox in US the C&C Server was in East coast

Allide.sys contained a rootkit that had more functionality and behaved like spyware, a new advanced version of BlackEnergy

OLOLO.exe performs search operations after which it writes Zero's to all targeted files (media files) and sents infected PC to restart cycle with already kileld MBR

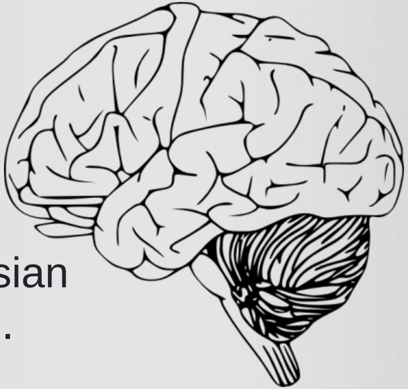
NEW VARIANT OF KILLDISK

KILLDISK AS RANSOMWARE

Ransom

- **Distructive KillDisk Malware Turns Into Ransomware**
- **The new functionality enables them to monetize their attack**

Who is the Brain?



- Developed by TeleBots gang, a group of Russian cybercriminals, evolved from Sandworm gang.
- Sandworm gang is responsible for sting of attacks in US, duing 2014. Also conducted Ukrain attack in Dec. 2015.
- The Telebots gang recently moved into cyber-sabotage attacks against Ukrainian banks.

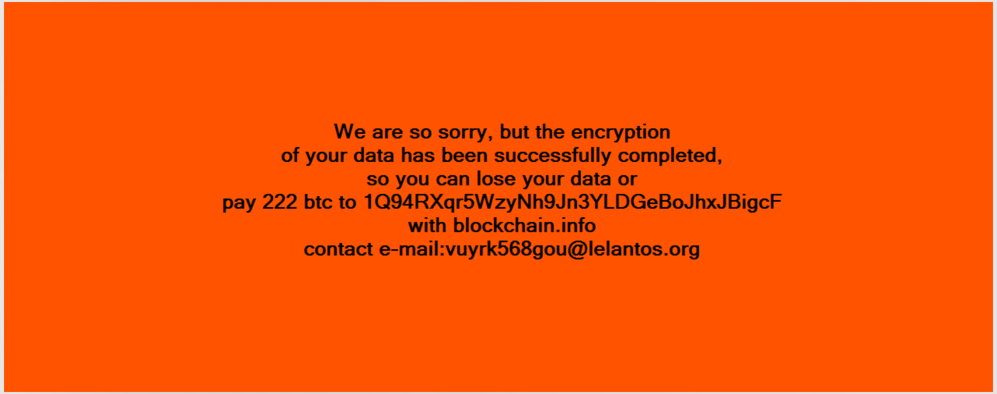
Who is the Target?

Organizations can be an ideal target for ransomware for several reasons:

- Physical safety risks and production outages
- Network operations typically cannot be easily shut down.
- Data backup processes may not cover all the required data.
- Employees of industrial organizations might be less aware of cyber threats.

> “Enterprises are more likely to quietly pay the ransom because of concerns that going public with cyberattacks will invite greater scrutiny from regulators, and possibly fines (environmental, safety, etc.),” said Phil Neray, VP of industrial cybersecurity at CyberX..

KillDisk demands a pretty high ransom:
222 Bitcoins (around US$170,000)



We are so sorry, but the encryption
of your data has been successfully completed,
so you can lose your data or
pay 222 btc to 1Q94RXqr5WzyNh9Jn3YLDGeBoJhxJBigcF
with blockchain.info
contact e-mail:vuyrk568gou@lelantos.org

How is it Done?

- Targets are Linux and Windows OS.
- Encryption keys are not saved anywhere on Linux, which makes it hard to recover files.
- On Windows each file is encrypted via an AES-256 key, and then further the AES keys are encrypted with a public RSA-1028 key.

How to Prevent?

- Create awareness within the organization
- Maintain back-ups that are rotated regularly

Questions:

Which of the following component(s) is/are not part of the Ukraine KillDisk Attack?

i)Tools & Tech
ii) Spearphishing and VPN Access
iii) Pharming and DDos

A) i) and ii) only
B) i) only
C) iii) only
D) None of the above

Answer: C

Questions:

How does Kill Disk (ololo.exe) cover its tracks after infecteing a computer and looking at files?

Answer:
It would erase any trail of its existence from the infected computer by writing zeroes to all files it was looking for.

Questions:

What type implentation was the KillDisk Ransomware based on?

- **CryptoLocker**
- **ScreenLocker**
- **Keylogger**
- **Logic Bomb**

Answer: CryptoLockers

References

https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf

https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/

https://www.wired.com/2016/01/everything-we-know-about-ukraines-power-plant-hack/

http://www.welivesecurity.com/2017/01/05/killdisk-now-targeting-linux-demands-250k-ransom-cant-decrypt/

https://www.bleepingcomputer.com/news/security/killdisk-disk-wiping-malware-adds-ransomware-component/

References

https://socprime.com/en/blog/dismantling-killdisk-reverse-of-the-blackenergy-destructive-component/

https://socprime.com/en/blog/results-of-initial-investigation-and-malware-reverse-analysis-of-fire-sale-ukraine/

http://www.welivesecurity.com/2016/01/04/blackenergy-trojan-strikes-again-attacks-ukrainian-electric-power-industry/

https://www.wired.com/2016/01/everything-we-know-about-ukraines-power-plant-hack/

http://www.thespec.com/news-story/6222551-russians-have-now-learned-to-hack-power-grids/

References

https://www.bleepingcomputer.com/news/security/killdisk-ransomware-now-targets-linux-prevents-boot-up-has-faulty-encryption/

http://thehackernews.com/2017/01/linux-ransomware-malware.html

https://securingtomorrow.mcafee.com/mcafee-labs/analyzing-killdisk-ransomware-part-1-whitelisting/

http://www.welivesecurity.com/2017/01/05/killdisk-now-targeting-linux-demands-250k-ransom-cant-decrypt/

http://www.computerworld.com/article/3155240/security/killdisk-evolves-into-ransomware.html