Tech Talk BSI UII

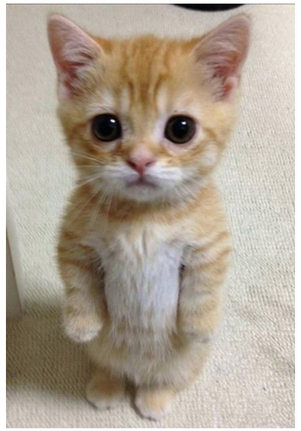
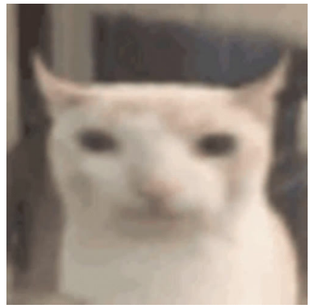
Dead Man's Switch

"dead man tell no tales, no more"

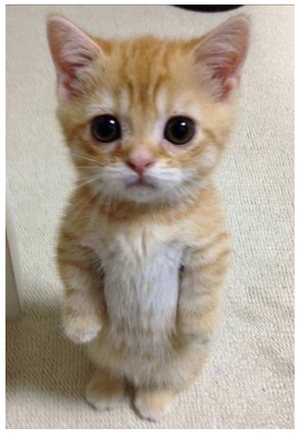
Vasant Paradissa Nuno Sakti

Outline

- Apa itu Dead Man's Switch
- Prinsip Kerja
- Penggunaan
- Demo
- Contoh di dunia nyata

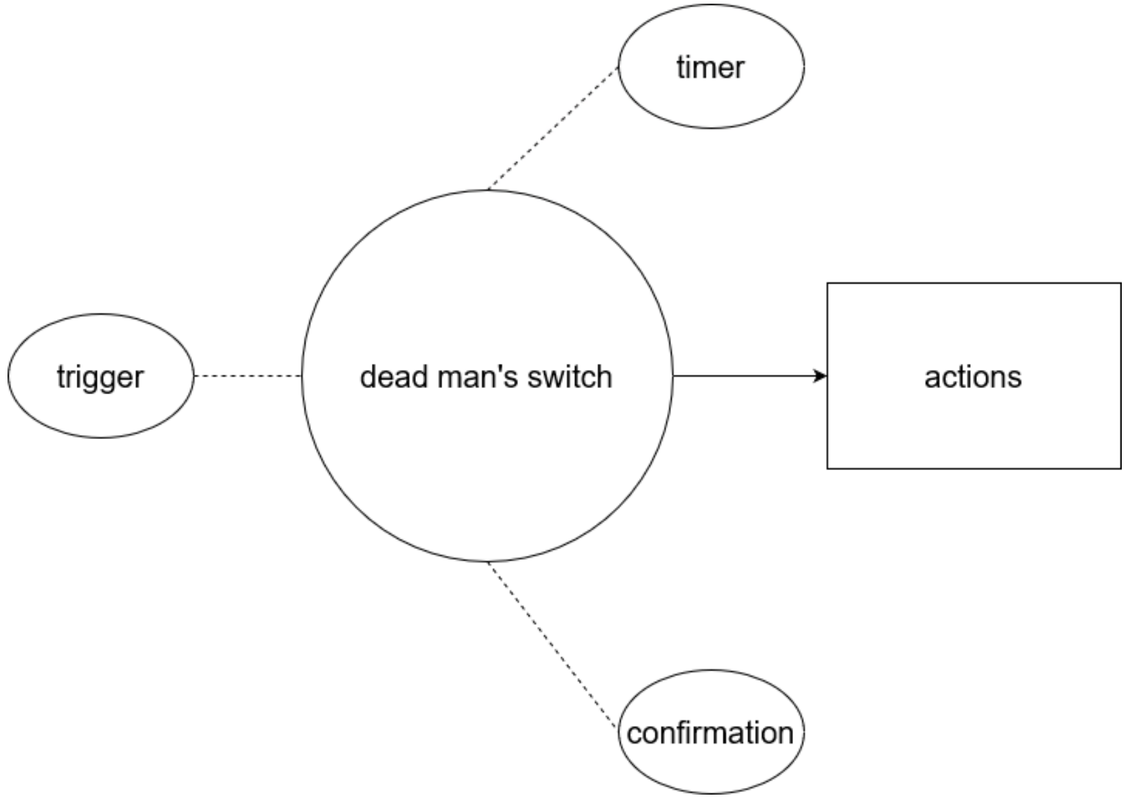




Apa itu "Dead Man's Switch (DMS)?"

- Pada intinya, DMS adalah mekanisme keamanan otomatis yang dirancang untuk diaktifkan ketika seseorang tidak mampu atau gagal melakukan suatu tindakan yang terjadwal.
- Konsep DMS berasal dari switch fisik yang digunakan dalam sistem transportasi, seperti kereta dan mesin, untuk memastikan kehadiran operator dan mencegah kecelakaan.
- Sekarang, DMS telah diadaptasi sebagai cara untuk melindungi data dan mempertahankan kendali terhadap aset digital.
- Switch ini dapat diimplementasikan dalam berbagai aplikasi dan sistem untuk memulai tindakan yang telah ditentukan ketika kondisi tertentu tidak terpenuhi.

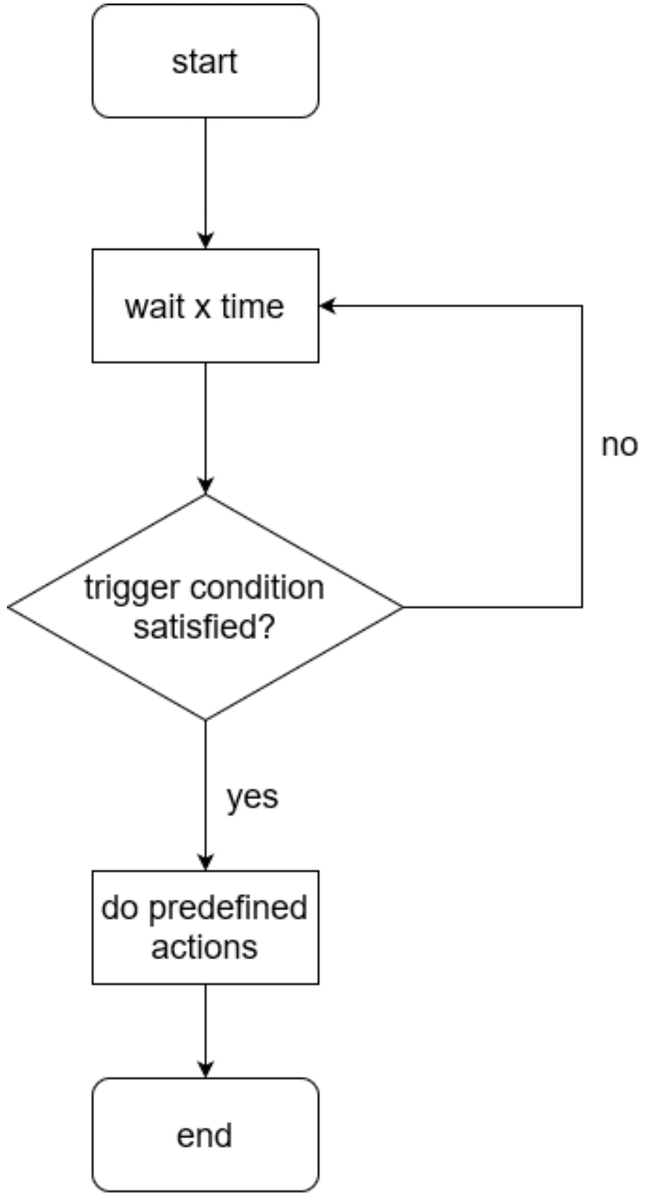

REVERSER



Contoh struktur:

- Pemicu (trigger): Kondisi yang mengaktifkan DMS.
- Timer: Pengatur waktu durasi pengecekan pemicu.
- Tindakan (action): Tindakan yang otomatis dilakukan jika DMS terpicu.
- Konfirmasi: Tindakan terjadwal untuk mencegah DMS terpicu.

Prinsip kerja



sederhana, tetapi efektif

Penggunaan

- Proteksi data dan privasi: melindungi data pribadi yang sensitif dalam situasi yang tidak terduga, seperti kecelakaan atau tidak aktif secara tiba-tiba (encrypt/delete). bisa juga merilis informasi penting, seperti surat wasiat, rahasia, atau credentials (passwords, keyfiles, cryptocurrencies).
- Pertahanan diri: A diancam oleh B karena mengetahui rahasianya. Tetapi B tidak mampu melakukan apapun karena A mempunyai sebuah DMS yang bisa merilis rahasianya.
- Software: Health check. Restart service atau mengalihkan request ke service lain jika suatu service unhealthy.
- Self-driving cars: Harus menyentuh stir setiap beberapa waktu.

Tindakan yang ditentukan bebas, termasuk tindakan tidak baik:

- Karyawan dendam ke perusahaan => buat DMS untuk hapus/bocorkan semua data saat namanya dihapus dari AD (hypotethical, misalnya).
- Sistem peluncuran nuklir otomatis sebuah negara saat negara itu menerima serangan nuklir.
- Handheld bomb trigger.

Demo

scenario: Kita ditangkap dan laptop bisa dicopy filenya oleh penangkap pake usb.

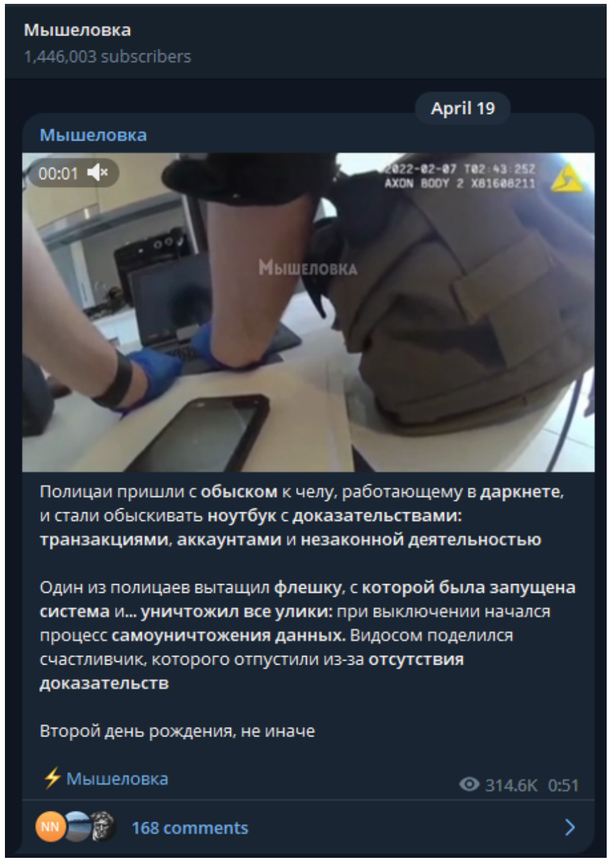
demo program:

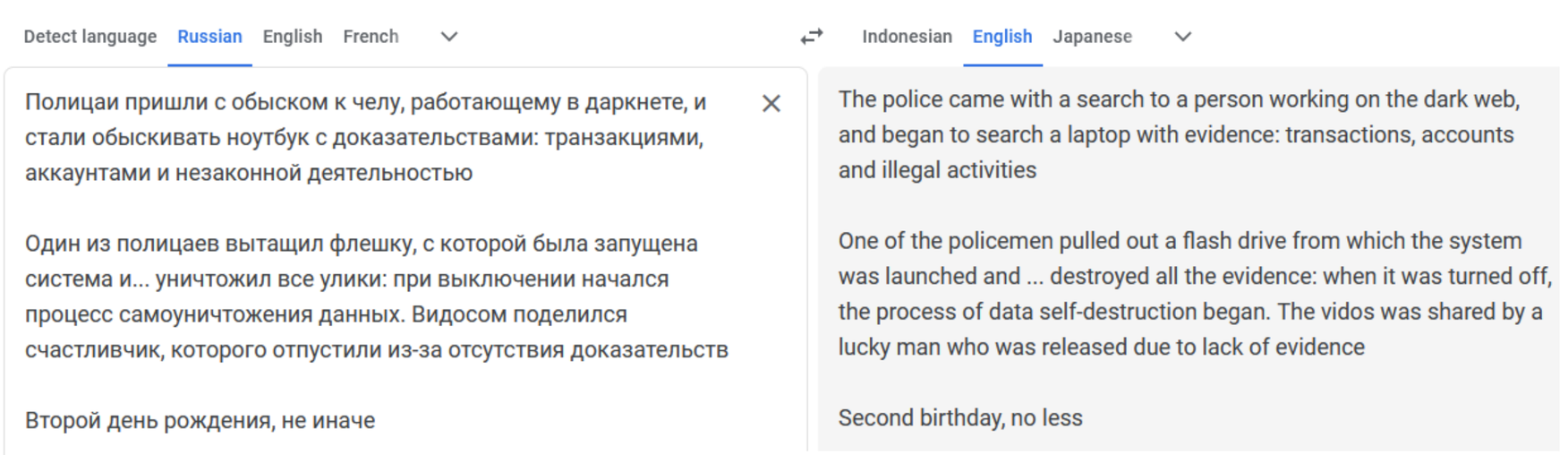
1. Get number of files in dev/bus/usb dir
2. Loop every 5s, check if number of files in the dir is the same
3. If number of files changes, delete secrets dir and post tweet

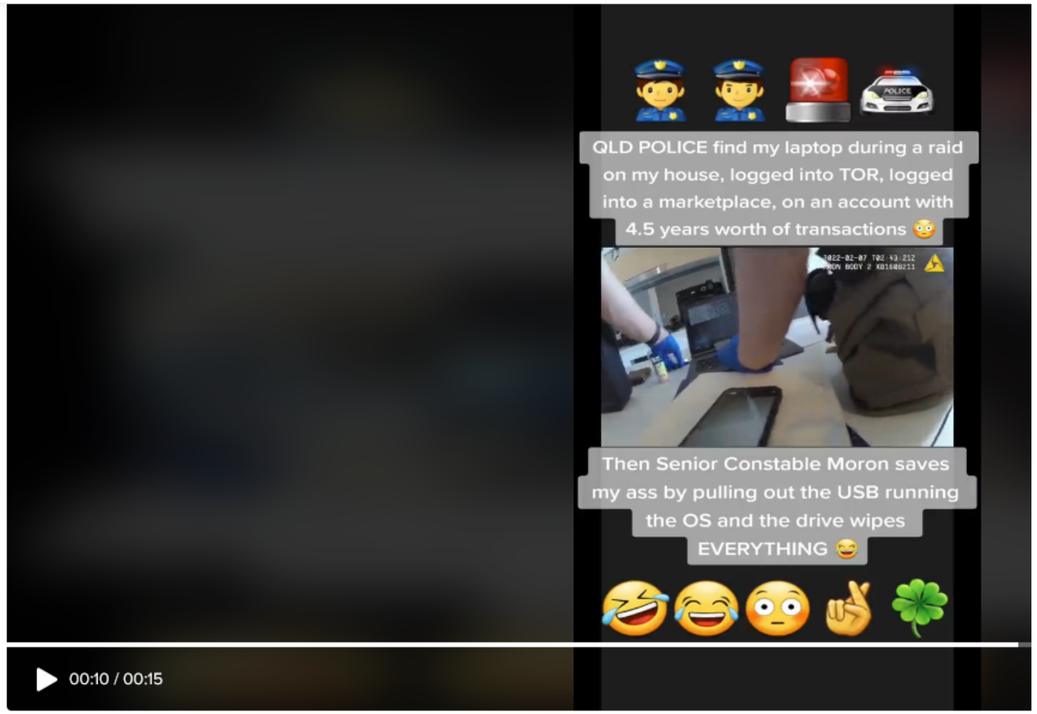
git: https://github.com/tsanva/dms

Contoh-contoh menarik (di dunia nyata)


-02-07 T02:43:112
AXON BODY 2 X81608211







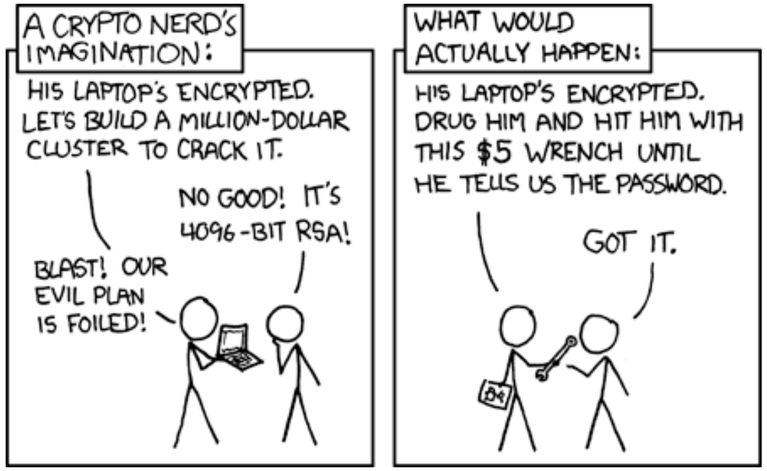
QLD POLICE find my laptop, logged into TOR, on the darkweb, logged into a marketplace...then this happens

#police #policeoftiktok #prison #qldpolice

Brisbane City

tools that might be used (from twitter post):

- kodachi/tails (installed on a usb flash drive)
- hephaest0s/usbkill
- starius/logic-bomb



more info:

https://graph.org/News-Proof-04-21 (links to telegram group and post)

https://twitter.com/officer_cia/status/1649305401064853504

https://www.reddit.com/r/hacking/comments/12uzp8o/that_is_why_utilizing_tails_os_and_whonix_os_in_a/

prequel + sequel and the video for full context:

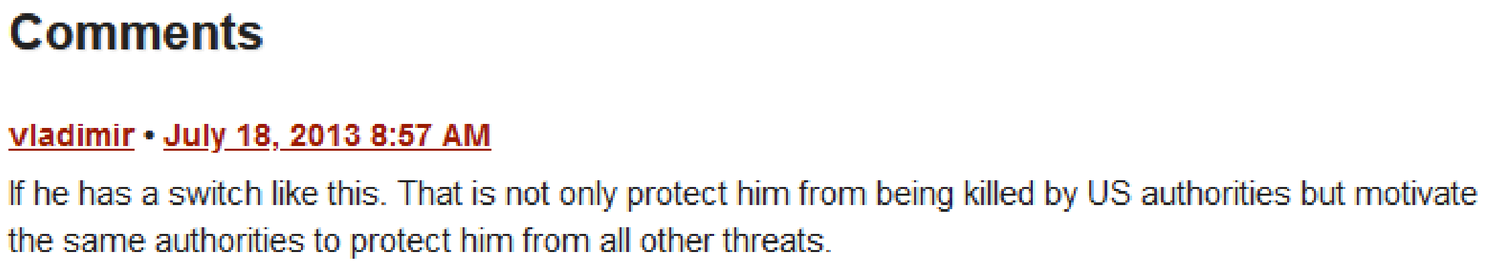
https://www.tiktok.com/@nygiffin/video/7222799407425572097

https://www.tiktok.com/@nygiffin/video/7217412645958225153

https://www.tiktok.com/@nygiffin/video/7230558179891940609

Snowden's DMS: 500 IQ move

(katanya) distribute copies of encrypted leaks -> release decryption key when he's incapacitated.



Comments

vladimir • July 18, 2013 8:57 AM

If he has a switch like this. That is not only protect him from being killed by US authorities but motivate the same authorities to protect him from all other threats.

Kalau dia terbunuh, rahasia US terbongkar. US jadi harus melindungi nyawanya (dari musuh yang ingin rahasia US terbongkar).

https://www.schneier.com/blog/archives/2013/07/snowdens_dead_m.html

tweet dihapus tidak lama setelahnya

more:

https://archive.org/stream/WikiLeaksFreedomForce/WL+Insurance+Thread_djvu.txt

https://www.wired.com/2013/07/snowden-dead-mans-switch/

https://archive.is/sDyiK

WikiLeaks

"Insurance files": File-file encrypted yang decryption key-nya akan dirilis saat terjadi hal yang tidak diinginkan. (seperti kasus Snowden)
Insurance files bisa didapatkan secara publik.

Why not just release all at once?
(katanya) Leaks dikurasi terlebih dahulu agar mudah dibaca.

USSR's Dead Hand

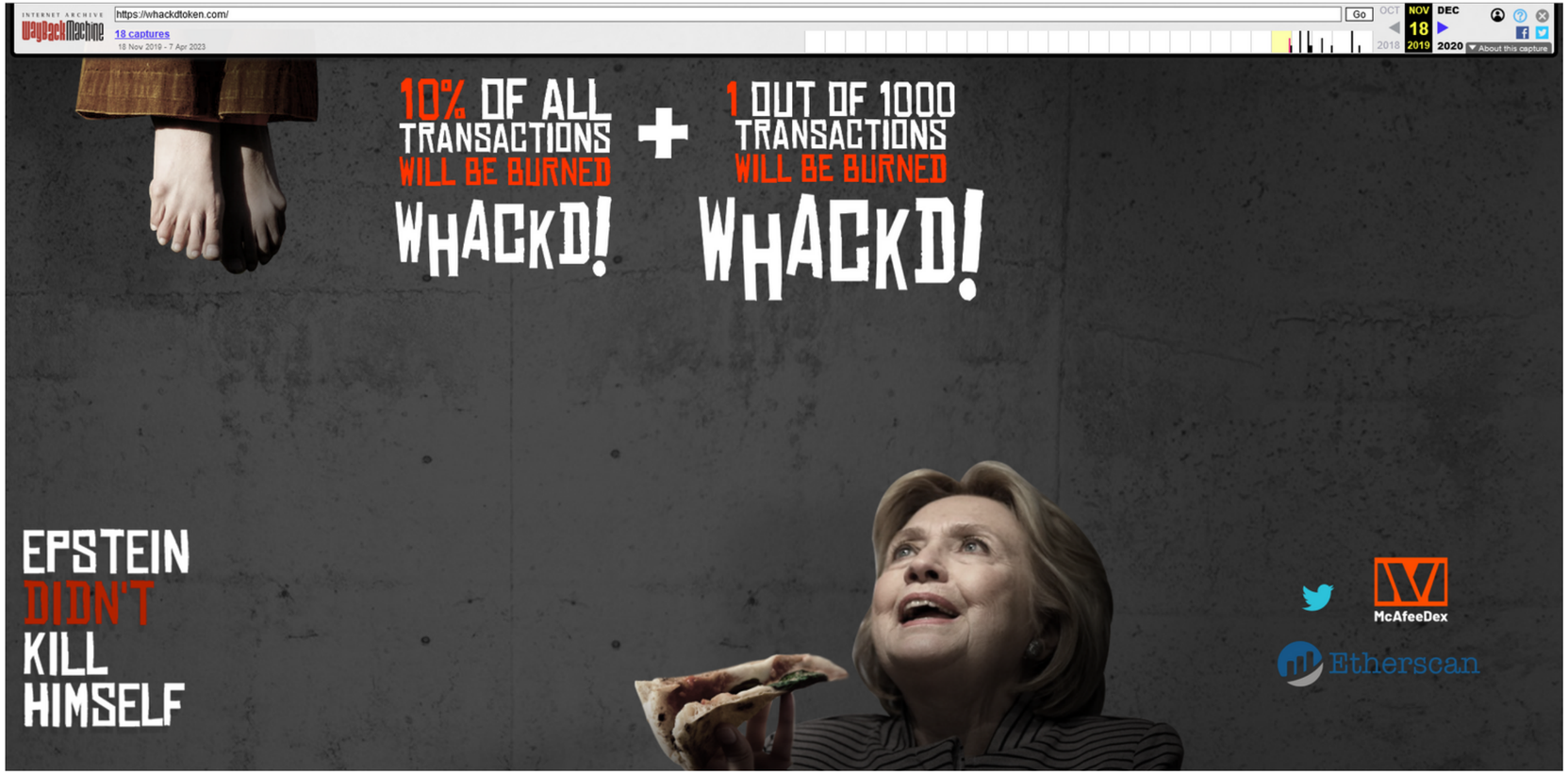
aka "Perimeter" System
"Mutual Assured Destruction", "Fail-deadly"

automatically initiate the launch of the Russian intercontinental ballistic missiles (ICBMs) by sending a pre-entered highest-authority order from the General Staff of the Armed Forces, Strategic Missile Force Management to command posts and individual silos if a nuclear strike is detected by seismic, light, radioactivity, and pressure sensors even with the commanding elements fully destroyed.

Negara-negara lain juga punya sistem yang mirip.

in pop culture: Dr. Strangelove (doomsday machine)

McAfee's $WHACKD



- airdropped 9000 $WHACKD ke fans (email, follower twitter) sebagai hadiah dari kubur?
- fixed value; unmineable

```
contract Epstein is ERC20Interface, Owned, SafeMath {
    string public symbol;
    string public  name;
    uint8 public decimals;
    uint public _totalSupply;
    uint random = 0;

    mapping(address => uint) balances;
    mapping(address => mapping(address => uint)) allowed;
```

```
function transfer(address to, uint tokens) public returns (bool success) {
    balances[msg.sender] = safeSub(balances[msg.sender], tokens);
    if (random < 999){
        random = random + 1;
        uint shareburn = tokens/10;
        uint shareuser = tokens - shareburn;
        balances[to] = safeAdd(balances[to], shareuser);
        balances[address(0)] = safeAdd(balances[address(0)],shareburn);
        emit Transfer(msg.sender, to, shareuser);
        emit Transfer(msg.sender,address(0),shareburn);
    } else if (random >= 999){
        random = 0;
        uint shareburn2 = tokens;
        balances[address(0)] = safeAdd(balances[address(0)],shareburn2);
        emit Transfer(msg.sender, to, 0);
        emit Transfer(msg.sender,address(0),shareburn2);
    }
    return true;
```

Mental Outlaw video: https://youtu.be/ls1Ekk763es

https://twitter.com/officialmcafee/status/1200864283766251521

Contoh proyek open source:

- BusKill (hardware + software, do stuffs when unplugged)
- hephaest0s/usbkill (shutdown, custom actions when unplugged)

Contoh app/service:

- Google Inactive Account Manager. Notify dan share data ke trusted contacts.
- www.deadmansswitch.net. Mengirim email ke beberapa orang.
- sarcophagus.io. Decentralized DMS application.

extra, contoh di anime:
Watari maintains a computer link to the orphanage he runs, and reports in at regular intervals. When Rem kills both him and L, at the proper time the computer reports "L is dead". This is a cue for the man currently operating the orphanage to send out L's successors, Near and Mello, to continue the Kira investigation.

https://tvtropes.org/pmwiki/pmwiki.php/Main/DeadMansSwitch

Kesimpulan

- DMS adalah sebuah mekanisme yang sederhana, tetapi efektif.
- Karena sifatnya yang sederhana, kita dapat membuat DMS kita sendiri untuk berbagai keperluan.
- Mekanisme DMS sudah banyak digunakan di dunia nyata, membuktikan kepercayaan terhadap kesederhanaan dan efektivitasnya.

Diskusi

some more sources:

- Cool blog post: https://nicholasjohnson.ch/2021/01/27/dead-mans-switch/
- https://en.wikipedia.org/wiki/Dead_man%27s_switch