Cold Boot Attack

Autor: Mateusz Lewczak

securitum

EDUKACJA PRZEDE WSZYSTKIM

securitum

Agenda

1. Ogólny zarys ataku typu Cold Boot.
2. Jak działa pamięć RAM na przykładzie DDR4.
3. Mechanizm Full-disk encryption na przykładzie BitLockera.
4. ATAK!!11!
5. Analiza uzyskanego zrzutu pamięci.
6. Jak się bronić?
7. Czy są inne fizyczne ataki na które trzeba uważać?

01

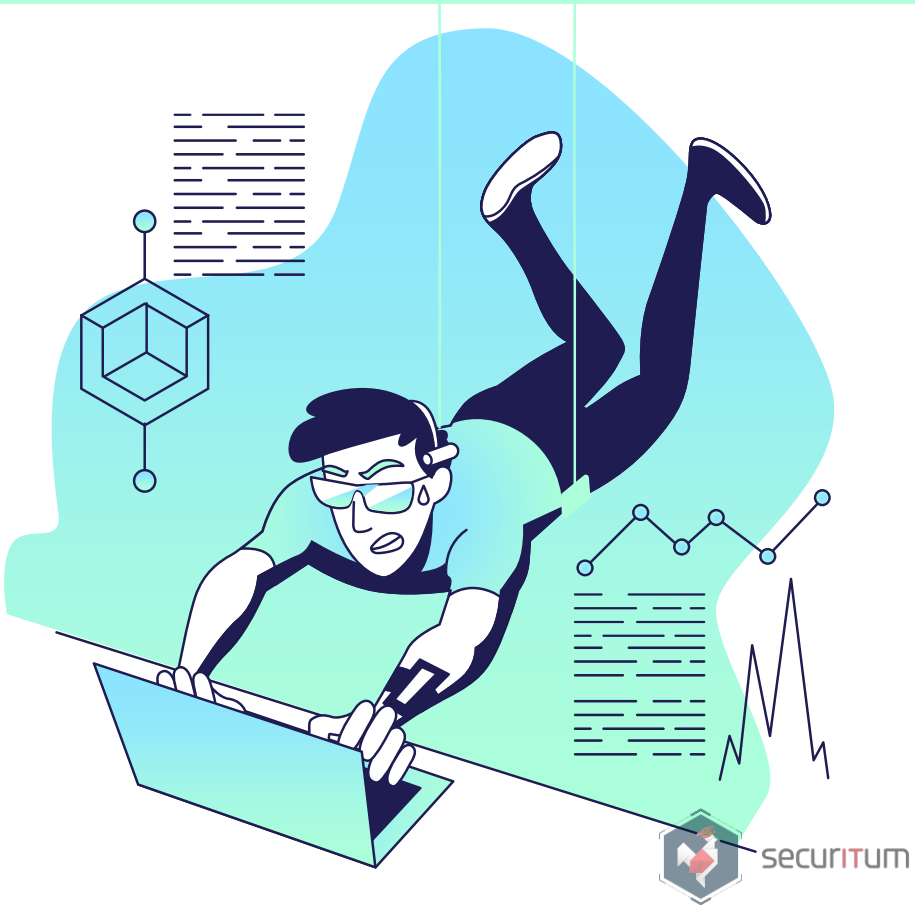
BIG PICTURE

Przebieg ataku

securitum

NASZA MISJA

1. Uzyskujemy dostęp do komputera ofiary.
2. Otwieramy obudowę.
3. Zamrażamy pamięć RAM.
4. Wyłączamy komputer.
5. Wykonujemy zrzut pamięci.

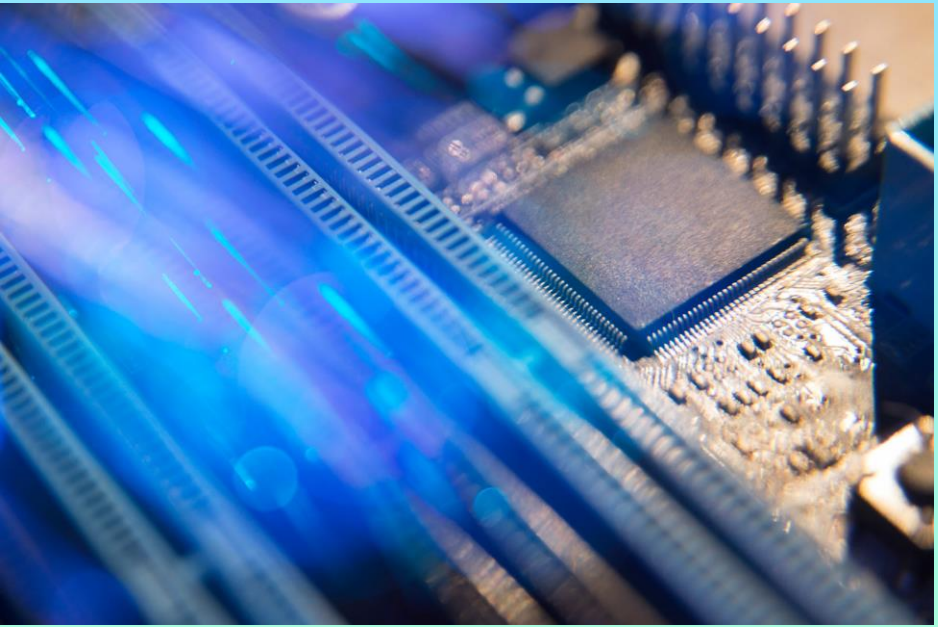


Dlaczego gaz zamraza?

„[...] Podczas iniekcji następuje obniżenie ciśnienia co prowadzi do przejścia cieczy w fazę gazową. Jednak analogicznie jak w przypadku wrzącej wody, aby ten proces mógł nastąpić potrzebne jest dostarczenie do substancji odpowiedniej ilości energii. Cała ta transformacja następuje gwałtownie, więc układ nie zdąży pobrać tej energii z otoczenia i musi wykorzystać swoją energię wewnętrzną, która jest związana z temperaturą substancji. Dlatego też gaz wydostający się z puszki jest zimny."

~ *dr Miłosz Panfil*

securitum

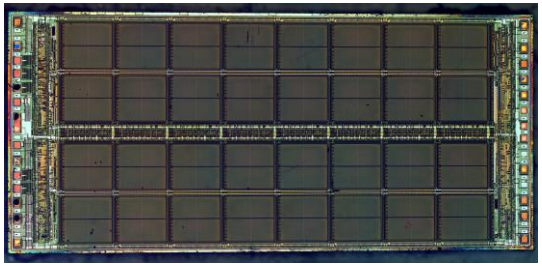


DLACZEGO JEST TO W OGÓLE MOZLIWE?

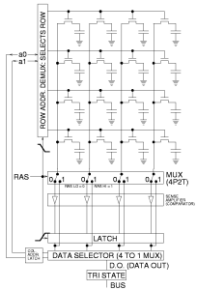
securitum

PAMIEC RAM

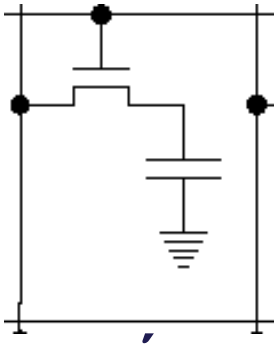
SODIMM



IC



KOMÓRKI

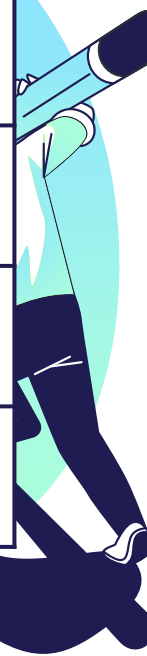


KOMÓRKA

securITum

CZAS I TEMPERATURA

MEM	Sekundy bez zasilania [s]	Procent błedów w temperaturze operacyjnej [%]	Procent błedów w temperaturze -50°C [%]
SDRAM 128Mb	60 300	41 50	(no errors) 0.000095
DDR 512Mb	360 600	50 50	(no errors) 0.000036
DDR 256Mb	120 360	41 42	0.00105 0.00144
DDR2 512Mb	40 80	50 50	0.025 0.18



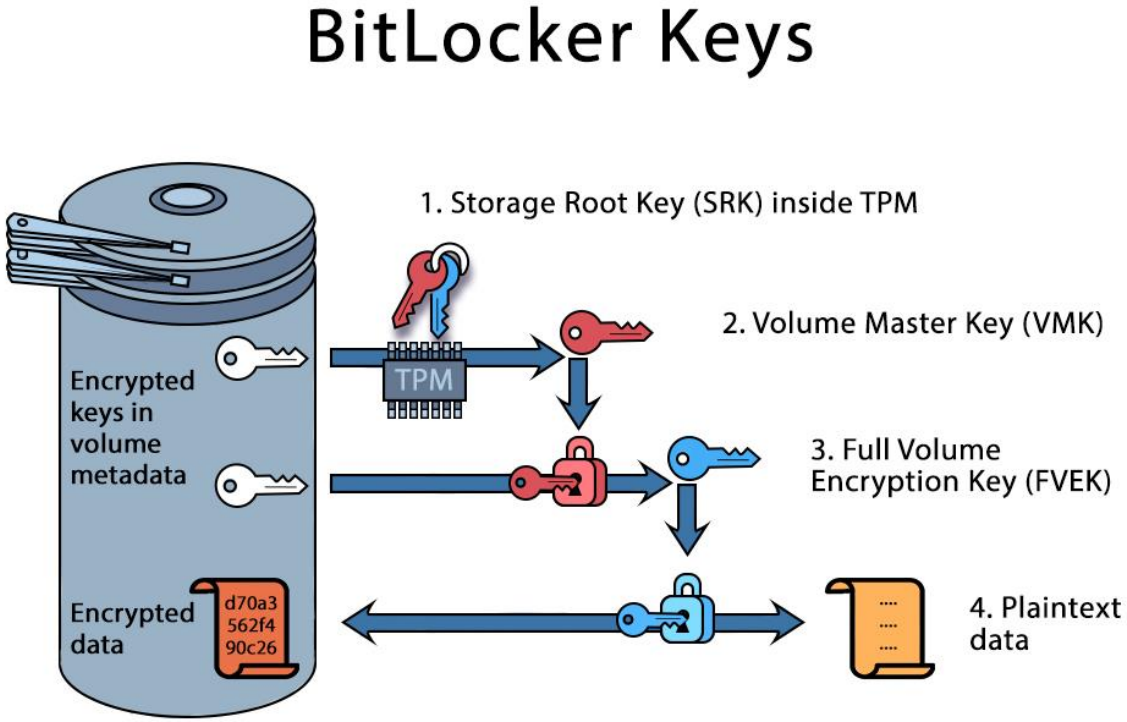
securitum

02

BitLocker

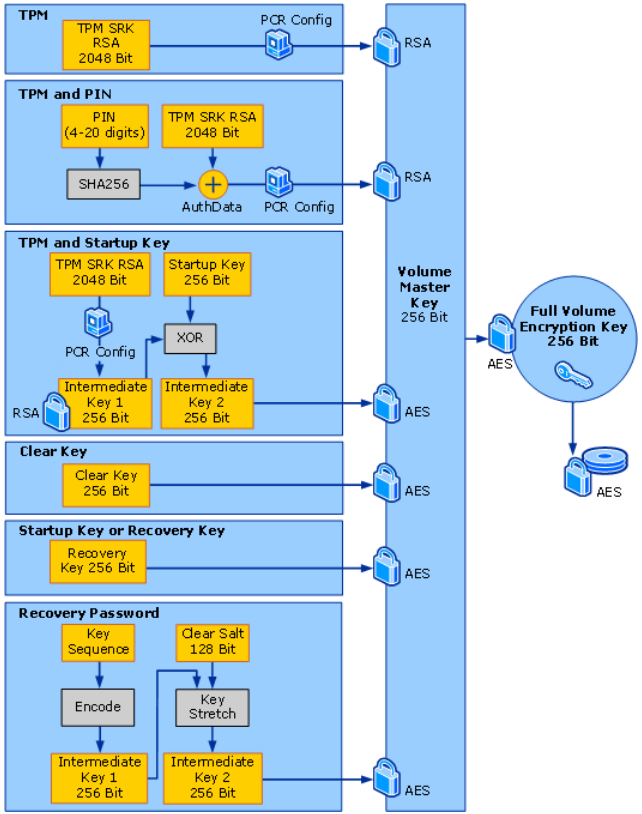
securITum

Prawda o kluczach



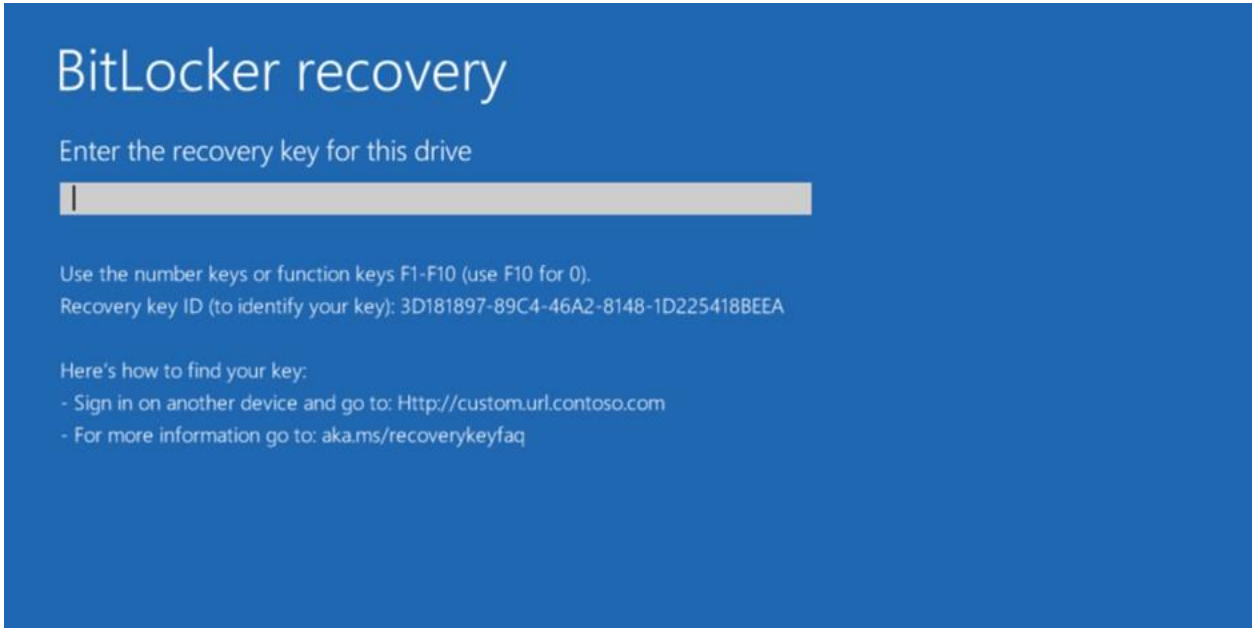
securitum

Prawda o kluczach



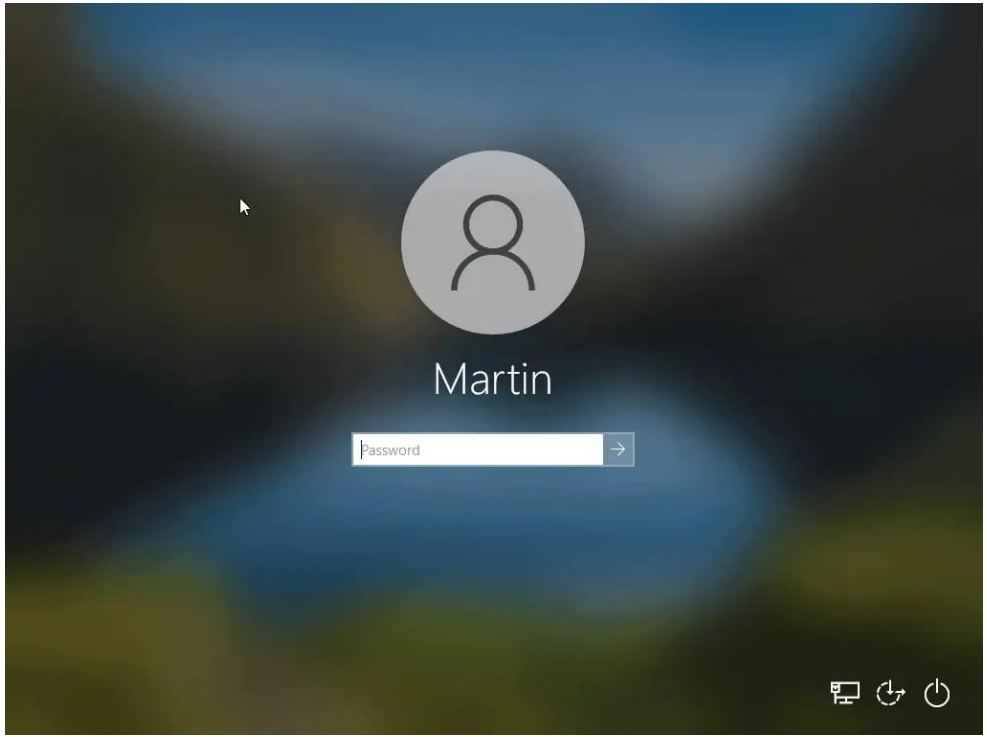
securitum

Wczesny etap rozruchu



securitum

Wczesny etap rozruchu cd.



securITum

Wczesny etap rozruchu cd.

„No, BitLocker doesn't encrypt and decrypt the entire drive when reading and writing data. The encrypted sectors in the BitLocker-protected drive are decrypted only as they're requested from system read operations. Blocks that are written to the drive are encrypted before the system writes them to the physical disk.”

~ Microsoft

Co poza BitLockerem?

1. Linux Unified Key Setup (LUKS)?
2. Wrażliwy jest każdy mechanizm, który trzyma klucze w pamięci!


PRZYGOTOWANIE

Potrzebny sprzet

1. 2x Sprężone powietrze w puszce.
2. *Pendrive USB.*
3. *Narzędzia potrzebne do otwarcia obudowy komputera.*
    1. *iFixit Pro Tech Toolkit.*
4. *Gaśnica.*
5. *Opaska antystatyczna.*
6. *Nitrylowe rękawiczki.*

securitum

Przygotowanie pendrive'a cz. 1

1. Pobranie i rozpakowanie memimage64

```
wget https://github.com/baselsayeh/coldboot-tools/releases/download/2/bios_memimage64.zip
unzip bios_memimage64.zip
cd bios_memimage64
```

2. Wgranie Master Boot Record na urządzenie

```
sudo dd if=grldr.mbr of=/dev/sdb conv=notrunc
```

securitum

Przygotowanie pendrive'a cz. 2

1. Utworzenie dwóch partycji

```
sudo fdisk /dev/sdb
> n
> [ENTER]
> [ENTER]
> +1G
> n
> [ENTER]
> [ENTER]
> +16G
> w
```

securitum

Przygotowanie pendrive'a cz. 3

1. Sformatowanie pierwszej partycji

```
sudo mkfs.fat /dev/sdb1
```

2. Zamontowanie partycji

```
sudo mount /dev/sdb1 /media/usb
```

3. Skopiowanie zawartości folderu bios_memimage64

```
sudo cp * /media/usb/
```

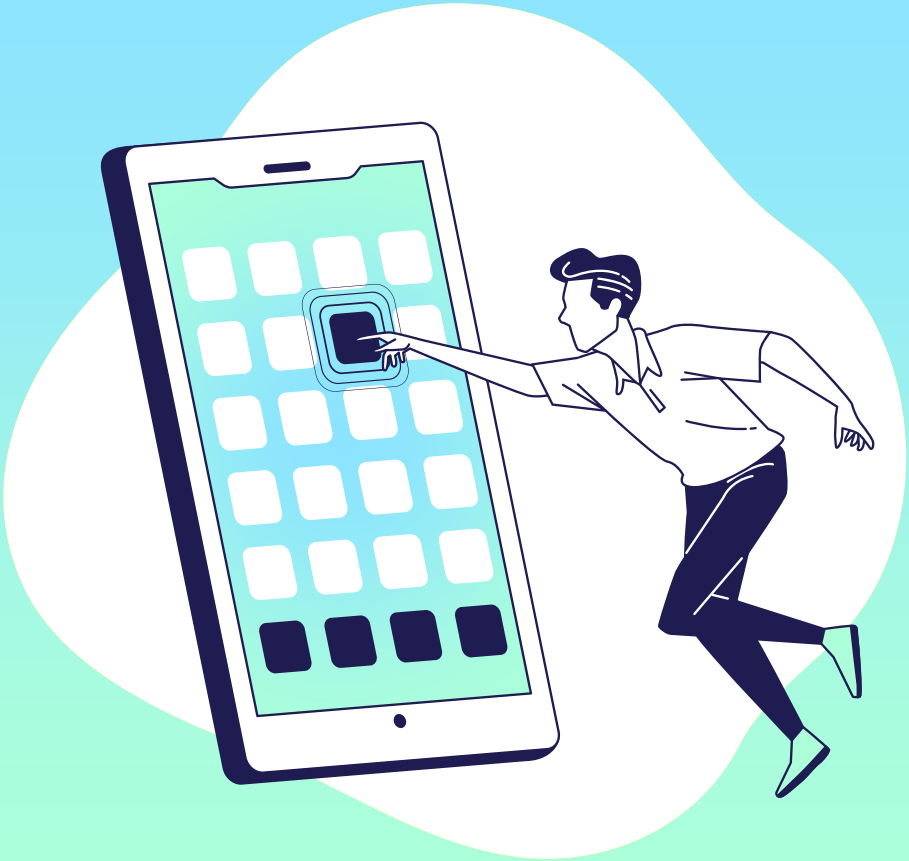
4. Odmontowanie partycji

```
sudo umount /media/usb
```

securitum

BEZPIECZEŃSTWO PRZEDE WSZYSTKIM

securitum



05
COLD BOOT TIME!

securitum

Mały disclaimer

1. BIOS vs UEFI.
2. Pamiętaj o kopii dysku.
3. GWARANCJA!!!

!!LIVE!!

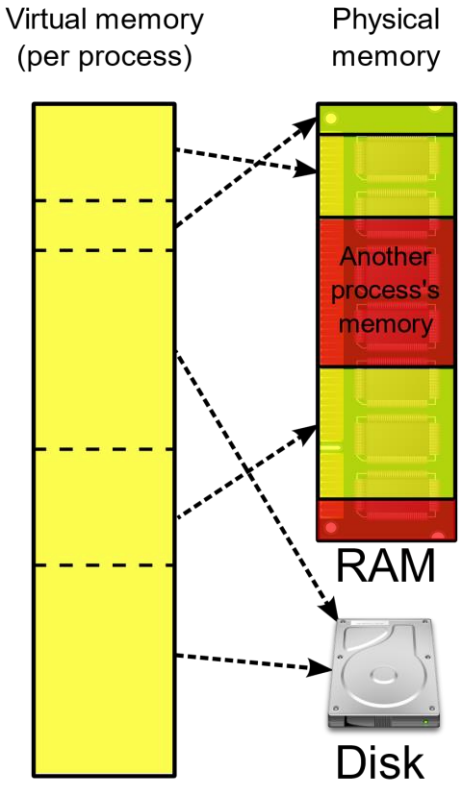
securITum

06

Analiza zrzutu

securitum

Jak faktycznie wyglada zrzut pamieci?



securitum

Co mozemy z niego wyciagnac?

1. Full Volume Encryption Key.
2. Hashe zalogowanych użytkowników.
3. Otwarte pliki.

Memory Forensic

1. Pule pamięci systemu Windows:
    1. None,
    2. Cngb,
    3. FVEc.
2. Właściwości kluczy AES.

Memory Forensic

1. Czego szukamy?
2. Jak to znajdziemy?

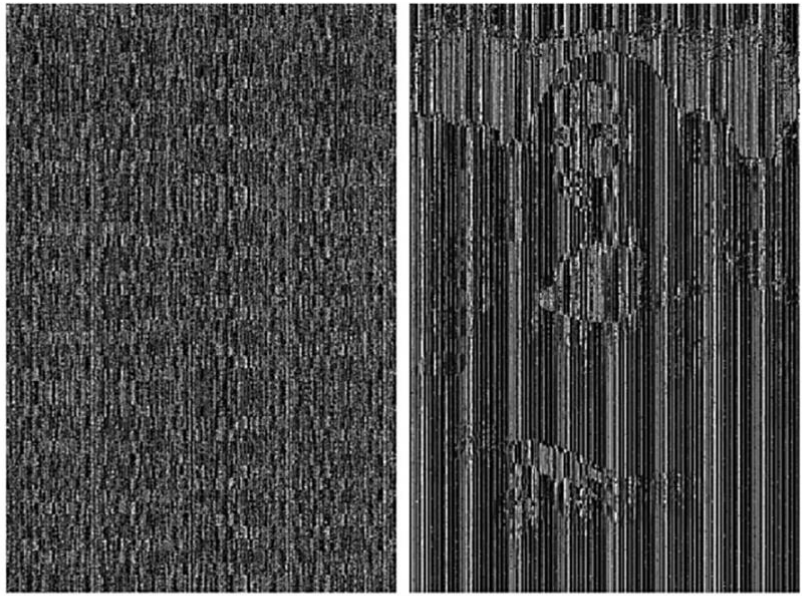
07

JAK SIE BRONIC?

Srodki prewencji

1. Nie zostawiaj laptopa bez opieki.
2. Wyłącz tryb uśpienia, korzystać z hibernacji.
3. Korzystaj z UEFI (domyślny Memory Scrambling).

Mona Lisa po scramblingu



(a) Scrambled image captured at +30 °C

(b) Scrambled image captured at -30 °C

Direct Memory Access Attack

1. PCI Express,
2. Thunderbolt 3.

SPI Sniffing

1. Zależy od implementacji FDE.
2. Głównie dotyczy BitLockera.
3. Co na to Microsoft?

INSPIRACJA

Komputer jest wyposażony w klasyczny BIOS, a nie UEFI. UEFI domyślnie w swoim standardzie wspiera funkcję, która na wczesnym etapie rozruchu wypełnia pamięć RAM losowymi danymi, aby utrudnić przeprowadzenie takiego ataku. Nie wyklucza to jednak scenariusza, w którym atakujący mógłby przenieść zamrożoną pamięć do innego komputera, który takiego zabezpieczenia nie ma.

W testowanym przypadku szyfrowanie dysku zostało ustawione z użyciem LUKS2, wykorzystując hasło. Co jest znacznie bezpieczniejszym rozwiązaniem niż obecnie zaimplementowana konfiguracja z automatycznym odblokowywaniem dysku. Pomimo najbezpieczniejszych ustawień w testowym urządzeniu, udało się pozyskać klucz Master Key z pamięci RAM urządzenia.

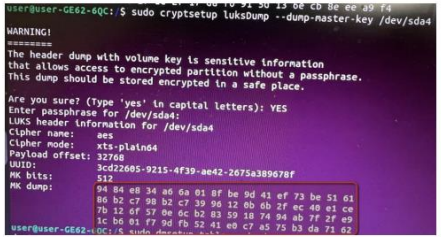
Warunki niezbędne do wykorzystania podatności

Fizyczny dostęp do maszyny docelowej. Komputer musi być odblokowany (po odszyfrowaniu, ale na ekranie logowania) lub mieć opcję automatycznego deszyfrowania dysku.

Szczegóły techniczne (proof of concept)

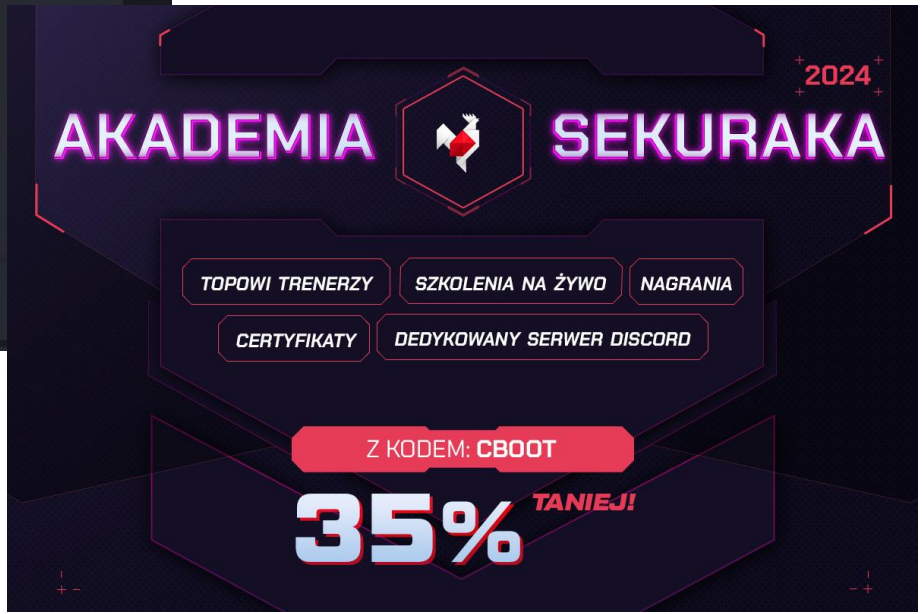
W celu przyspieszenia ataku założono znajomość Master Key wykorzystywanego do deszyfrowania dysku. Można go uzyskać za pomocą poniższej komendy w terminalu:

```
# cryptsetup luksDump --dump-master-key /dev/sda4
```



securitum

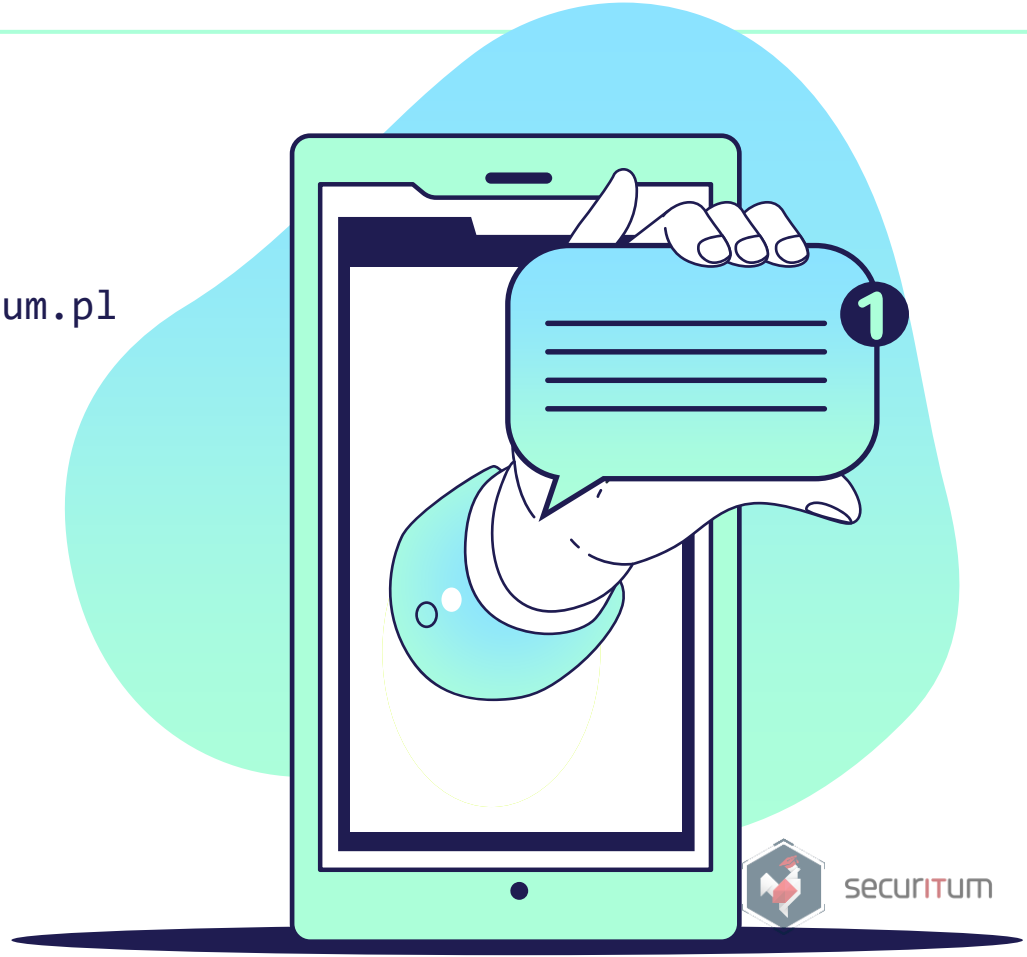
KOD PROMOCYJNY



DZIEKI!

Pytania?

Email: mateusz.lewczak@securitum.pl
GH: LeftarCode



securitum

Bibliografia

1. DLACZEGO ROZPRĘŻANIE GAZU PROWADZI DO OBNIŻENIA TEMPERATURY?
   https://zapytajfizyka.fuw.edu.pl/pytania/dlaczego-rozprezanie-gazu-prowadzi-do-obnizenia-temperatury/
2. Lest We Remember: Cold Boot Attacks on Encryption Keys
   https://www.usenix.org/legacy/event/sec08/tech/full_papers/halderman/halderman.pdf
3. Lest we forget: Cold-boot attacks on scrambled DDR3 memory
   https://www.johannes-bauer.com/personal/publications/2016-03-Bauer-DFRWS-EU.pdf
4. Recovering BitLocker Keys on Windows 8.1 and 10
   https://tribalchicken.net/recovering-bitlocker-keys-on-windows-8-1-and-10/
5. Plugin do Volatility
   https://github.com/elceef/bitlocker/blob/master/bitlocker.py
6. Radare2
   https://github.com/radareorg/radare2
7. Dislocker
   https://github.com/Aorimn/dislocker

securitum