Briefing document

How Secure are TPM Chips?

CovertSwarm

CONTENTS

01. FULL DISK ENCRYPTION IS NO LONGER ENOUGH

This briefing document demonstrates that the security of BitLocker for full disk encryption - when deployed in conjunction with Trusted Platform Module (TPM) - is no longer enough to effectively ensure the confidentiality of that encrypted data.

02. CAN YOU HACK TPM CHIPS? YES

Organisations that employ these technologies should consider CovertSwarm's findings and review the associated information security risks and their impact upon their security posture.

We acknowledge and expand upon the TPM work carried out by Henri Nurmi at F-Secure [1], to demonstrate a real-world attack chain against Microsoft's BitLocker full disk encryption. Our simulated breach was performed during the Summer of 2021 against one of CovertSwarm's clients subscribed to our flagship Constant Cyber Attack service.

03. EXTRACTING BITLOCKER ENCRYPTION KEYS FROM TPM TO DECRYPT FULL DISK CONTENTS AND ESCALATE PRIVILEGES

WE WILL EXPLAIN HOW:

1 From a fully encrypted device - we not only obtained the BitLocker key from the device's TPM but then proceeded to access the full disk contents that allowed us to escalate privileges upon the device.

2 We will also delve into some of the difficulties experienced – and workarounds - that were made

04. BACKGROUND

One of our Constant Cyber Attack clients directed our swarm to the scenario of a corporate laptop being stolen, asking the following:

“What would be possible in the hands of a hacker or malicious individual?”

This client has had numerous Penetration Testing engagements previously and implemented hardening of their Windows laptop builds using industry-standard ‘best practices’ such as device lockdown and full disk encryption via BitLocker.

CovertSwarm exists to constantly compromise our clients, therefore we wanted to simulate how a real-world threat actor might approach and fully exploit such a situation with their aim to gain access to the encrypted disk contents and take complete control of the device to in-turn use this to further breach our client.

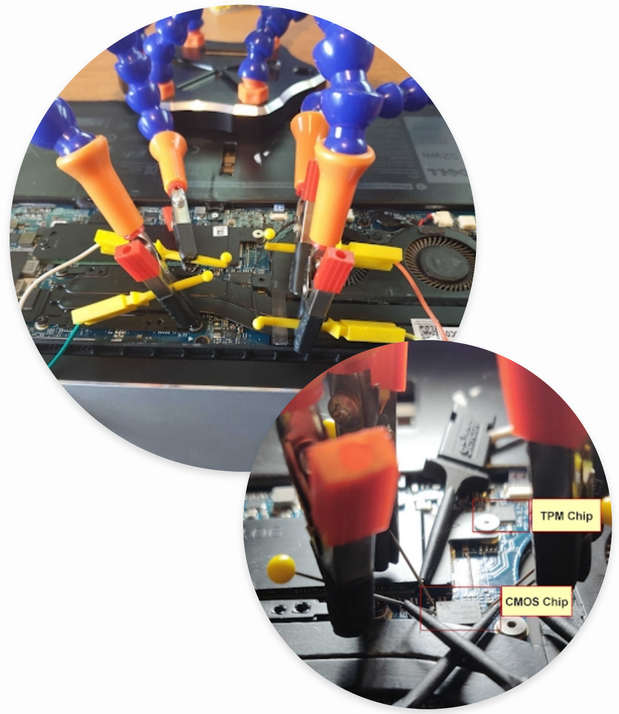
We enacted a staged theft of one of their modern Dell XPS 9370 laptops running Windows 10 Professional, which housed a TPM 2.0 chip and set to work.

CovertSwarm

05. WHAT IS A TPM CHIP AND WHAT DOES IT DO?

Trusted Platform Module (TPM) is a secure cryptoprocessor that is designed to carry out cryptographic operations to authenticate users. Additionally, a TPM can attest that the host system has not been compromised or been modified whilst offline.

The TPM achieves this by monitoring the boot process and measuring these results or ‘secrets’ within a Platform Configuration Register (PCR).



05. TPM BEHIND THE SCENES

TPM currently has two versions 1.2 and 2.0. TPM 1.2 was released in 2005, and the most recent revision it received was in 2011. TPM 2.0 was first released in 2014, with the most recent revision being in 2019.

The TPM 2.0 specification is a "library specification", which means that it supports a wide variety of functions, algorithms, and capabilities upon which future platform-specific specifications will be based. One of the primary differences between 1.2 and 2.0 is the supported hashing algorithms and functionality that the chip itself can support, for example, TPM 1.2 only employs the insecure SHA-1 hashing algorithm, whereas TPM 2.0 supports SHA2-256.

BitLocker's main objective is to protect user data at rest and upon the protected volume of the host's hard drive. To achieve this, disk sectors are encrypted with a Full Volume Encryption Key (FVEK), which is always encrypted with the Volume Master Key (VMK), which, in turn, is bound to the TPM. The VMK directly protects the FVEK and therefore, protecting the VMK becomes critical. By storing these encryption keys in the TPM along with a reference to a specific PCR state, data can be effectively locked.

The keys are only unlocked and released once the state of the system is validated against the stored PCR values, ensuring that encrypted systems can only be accessed if specific hardware or software conditions are met.

BitLocker can be configured to use additional protectors in the form of a numerical PIN number, USB start-up key, or both PIN and USB start-up key, which is used to further protect the VMK. When these additional protectors are in place the TPM will require extra information before unsealing the VMK.

It should be noted that an attack could still obtain the key however this capture would need to occur at the same time as the PIN is entered. Without the use of these protectors, the decryption process starts automatically exposing the VMK.

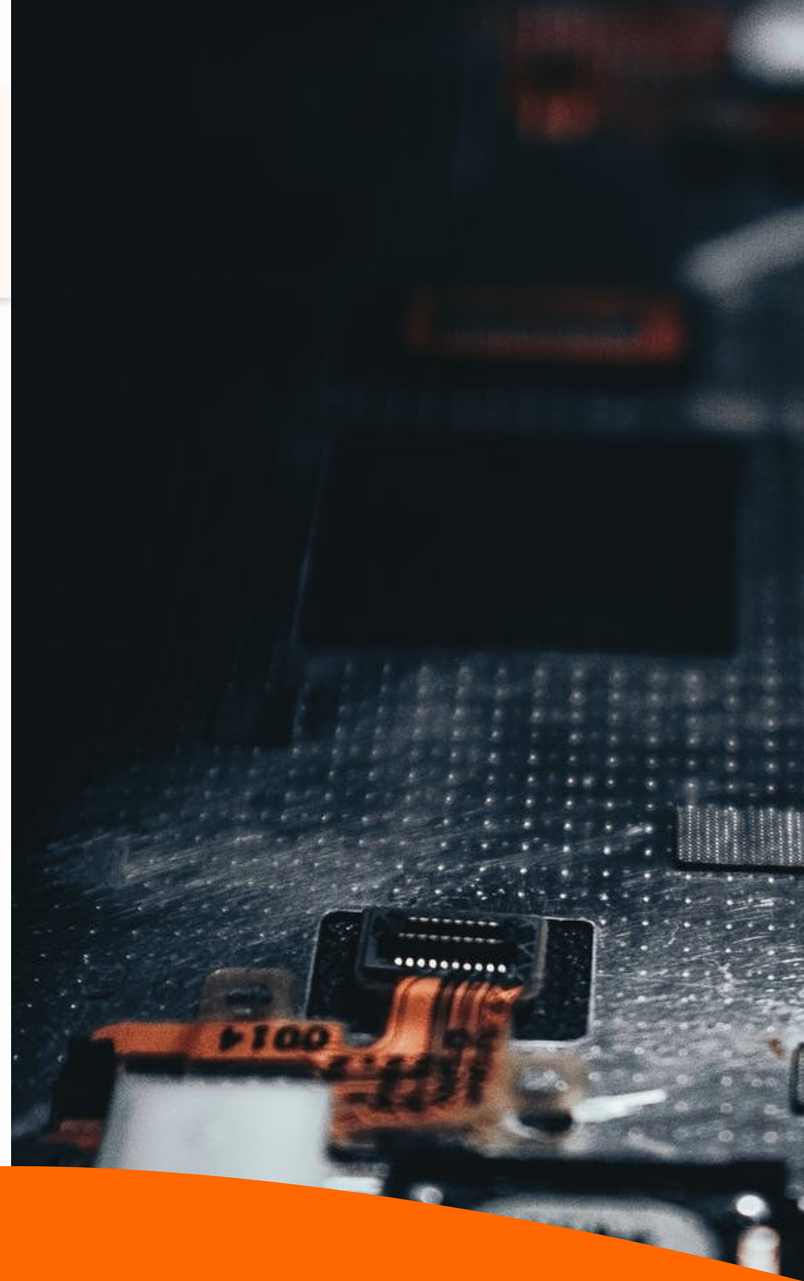
Previous research has highlighted that by default the TPM traffic is not encrypted when the TPM is communicating with the CPU, which allows for electronic signals to be captured - or 'sniffed' - during its operation.

06. METHODS OF EXTRACTING DATA

During our investigation several differing TPM chips and vendors were identified [1] which have a documented SPI interface [2]:

SPI, or Serial Peripheral Interface, is a synchronous serial communications interface supporting full-duplex communication with high-speed clock frequencies. It uses master-slave architecture, where the master device always initiates the communication.

Modern computers often have these common IC (integrated circuit) packages included within their motherboard design; however, several aftermarket options are available.



06. METHODS OF EXTRACTING DATA

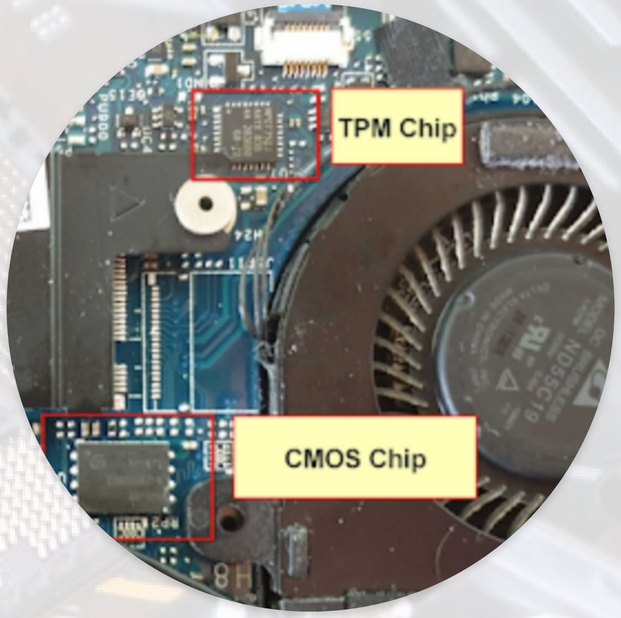
Two common packages breakdowns as per the images. There are several pins that were of interest to our attack scenario that was specifically related to the SPI protocol.

SPI_CLK	MOSI	MISO	SPI_CS
Serial Clock	Master Out Slave In	Master in Slave Out	Chip Select

06. METHODS OF EXTRACTING DATA

The form-factor of the TPM chip within the 'stolen' laptop we focused our attack upon inhibited the trivial extraction of its data due to the chip's location and size presenting us with difficulty when connecting a Logic Analyser device (described later) to its physical pins. That said, with sufficient time we found this to be achievable and we were ultimately able to connect to the TPM chip from an external source.

A shortcut to this means of connection was found to be possible through our identification of the laptop's CMOS flash chip that was located on the same physical trace bus as the TPM - which connects both to the CPU via the SPI (Serial Peripheral Interface) protocol. Additionally, the CMOS chip was more easily accessible due to its somewhat larger size (vs TPM) and its reduced number of pins.



06. METHODS OF EXTRACTING DATA

As the SPI bus communicated openly between the TPM and CMOS chips the aim was to capture signals both destined to and sourced from the TPM by connecting to the CMOS pins as a physical proxy.

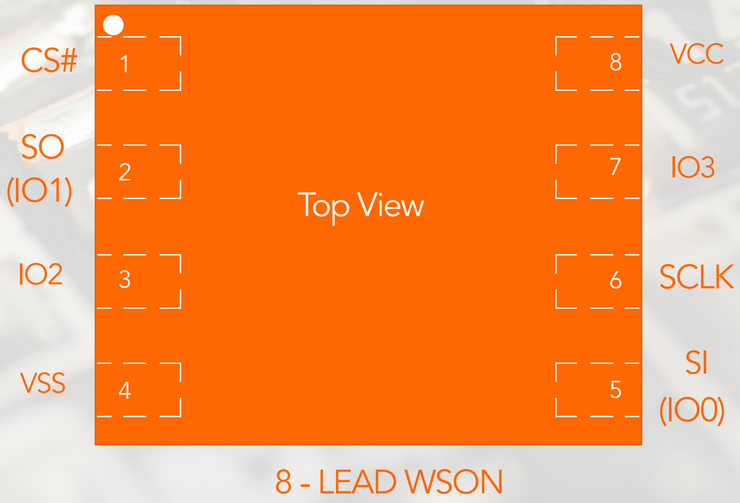
In respect of this attack, the key SPI interfaces of the CMOS chip consisted of four input/output signal connections:

Enable
Enable (Pin 1)

MISO
Master in Slave out (data from the slave) (Pin 2)

MOSI
Master out Slave in (data from the master) (Pin 5)

SCLK
Serial Clock (Pin 6)



8 - LEAD WSON

06. METHODS OF EXTRACTING DATA

The layout of the chip connections was identified through publicly accessible information in the form of product datasheets:

To extract the VMK from the TPM, a “side-channel attack” would need to take place. During this attack, a malicious actor would require physical access to the laptop, in addition to a Logic Analyser device.

A Logic Analyser is a device that is capable of capturing and displaying multiple signals from a digital system or circuit.

It may convert the captured data into timing diagrams, protocol decodes, state machine traces, assembly language, or may correlate assembly with source-level software.

07. SETUP & EXECUTION

We began by connecting the logic analyser to the CMOS chip and configuring the capture software (Logic2 [3]) to record data based upon the specified pin layout.

Of note is that the enable signal needed to be inverted due to the connection being established via the CMOS chip rather than the TPM chip, where the latter is specified as being a low enable signal. An actual attack could take seconds to perform, but due to the small form factor of the CMOS chip an IC test clip could not be connected, and the pin connection had to be fabricated using alternative, bespoke tools and connectors. We found that smaller form factor test clips are available for purchase, and varied in size and configuration and so could be obtained by an attacker attempting to complete this attack more quickly.

Once the physical connections were established it was possible to then initiate a stream capture of the signals via the logic analyser, and so we powered on the laptop.

Using publicly accessible tools which included a custom high-level analyser [4], and a script to enable the parsing of the captured data, it was possible to decode and extract TPM transactions from the SPI stream. This resulted in a data dump that we were then able to use as a search repository.

As discussed above, the architecture of BitLocker involves multiple keys: one of which is the Full Volume Encryption Key (FVEK) which is used to encrypt the BitLocker-protected volume. This key is encrypted by a Volume Master Key (VMK), and the encrypted FVEK is stored in the metadata of the volume.

Decoding the signal communications to TPM allowed the addresses and the data packets to be determined. The TPM register TPM_DATA_FIFO_0, as defined by the TPM specification, is used during the relay of the BitLocker key. This analysis was based upon various sources, which includes the research performed by F-Secure

07. SETUP & EXECUTION

From a manual recovery perspective, without using a script, the VMK can be identified as the 64 characters following the initial command input of 2C000000010000000320000, which is the specific command for the type and configuration of the VMK.

Filtered view showing the command and resulting BitLocker VMK as displayed here.

The recovery of this using an analyser script can provide trivial access to the VMK without manual review.

Data

tpm_data_fifo_0

Type	register	addr	data
read	TPM_DATA_FIFO_0	d40024	80
read	TPM_DATA_FIFO_0	d40024	01
read	TPM_DATA_FIFO_0	d40024	00
read	TPM_DATA_FIFO_0	d40024	00
read	TPM_DATA_FIFO_0	d40024	00
read	TPM_DATA_FIFO_0	d40024	0a
read	TPM_DATA_FIFO_0	d40024	00
read	TPM_DATA_FIFO_0	d40024	00
read	TPM_DATA_FIFO_0	d40024	00
read	TPM_DATA_FIFO_0	d40024	00
read	TPM_DATA_FIFO_0	d40024	80
read	TPM_DATA_FIFO_0	d40024	02
read	TPM_DATA_FIFO_0	d40024	00
			00

08. PROBLEM SOLVING

During this exercise, several problems were found which prevented the rapid extraction of the key.

Initially, it was not possible to capture the SPI data using a cheaper accessible Logic Analyser. This was primarily down to the available capture rate.

Due to the size of the TPM IC, connecting directly to the chip was difficult, however, it is possible to purchase several sized IC Test clips which would speed up the extraction process tremendously.

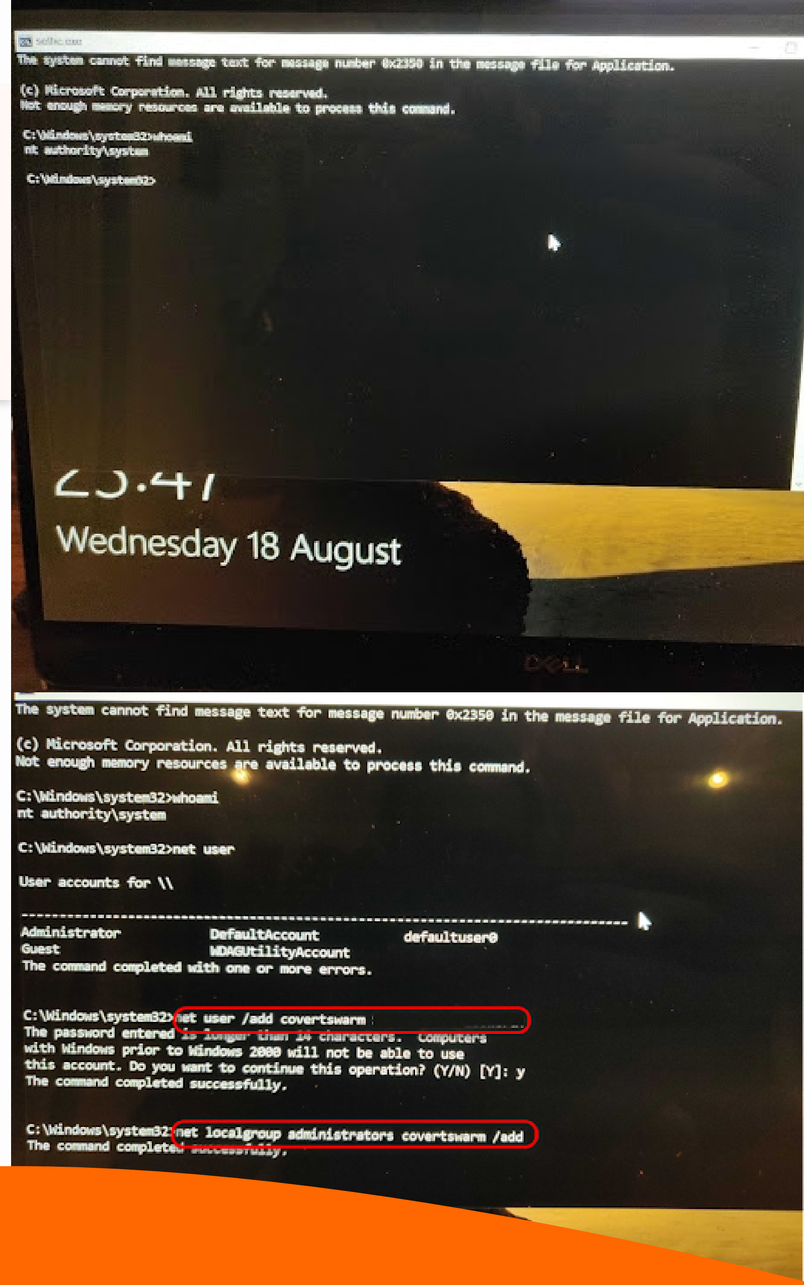
A second observation was that where although some TPM data appeared it was not possible to extract the VMK. After some investigation, it was found that grounding the laptop with the power cable resolved this and instantly allowed for the VMK to be extracted.

We found that changes to the internal hardware put the TPM into its Lockdown state where it required a recovery key to proceed. An example of such a change is disconnecting some motherboard components or the mainboard battery.

09. DECRYPTION AND PRIVILEGE ESCALATION METHODS

As the disk was mounted it was possible to read and extract local information such as the local Administrator password hash.

It was also found to be possible to make changes to the system to ensure persistent access, for example replacing sethc.exe with cmd.exe which allows the accessibility option “Sticky Keys” to be abused by supplying local SYSTEM level access on a locked host.



10. RECOMMENDATIONS AND MITIGATIONS

At the time of writing this briefing document, this attack chain cannot be fully mitigated on Windows devices encrypted with BitLocker using TPM. That said, it is possible to make genuine attacks slightly more challenging by taking a small number of steps to help reduce their chances of success:

TPM 2.0 devices support command and response parameter encryption, which would prevent the sniffing attacks, however, BitLocker does not support this feature currently as found in previous research. We will update this article once this support is available.

Using a second mechanism such as a PIN, Start-up Key, or - as recommended by Microsoft - both a PIN and Start-up key, in addition to disabling standby mode ensuring the device is shut down or hibernated would be key defences.

Note: the use of a PIN is only part of a solution as does not mitigate this attack fully.

For example, someone who knows the PIN could use this attack to escalate their own privileges on their own laptop locally – i.e. think of the insider threat and malicious employee scenarios.

Further, if the attacker obtains the PIN via another means, via a 'chained attack' such as social engineering or the employee made a physical note of the PIN somewhere for the attacker to access (think Post-it notes!) then again, this attack is still entirely possible

This is equally true if you consider the ability of an attacker to simply brute-force the PIN entry.

Standard controls, such as the use of a BIOS password can help to prevent changes to the BIOS from taking place.

10. RECOMMENDATIONS AND MITIGATIONS

During our research and successful exploit, we found the BIOS configuration to be open and accessible and so it permitted us to reconfigure the host to boot from an alternative device, such as a live USB. From there we were then able to then read and write to the hard drive.

It should be noted that even when set, CovertSwarm is aware of several methods by which to bypass/clear BIOS passwords as such a control.

Review your physical security controls, especially for highly sensitive data environments. Ask “does that device, or its held data, really need to leave our location?” As we have demonstrated, it may be encrypted but in the right (or wrong) hands this risk mitigation can be bypassed and the system is still breached.

Consider limiting or preventing local storage of any sensitive (especially classified) data, wherever practically possible.

11. CLOSING THOUGHTS

If your risk register accepts a risk due to a control-based around TPM and BitLocker then CovertSwarm's research and team advises that it be time to review that risk as a priority.

In this briefing document we have demonstrated how you can obtain a 'stolen' laptop, extract the encryption key, access disk contents, and escalate privileges to gain complete control of a device.

12. ABOUT US

Breaking into the world's most progressive brands. Every day

The team at CovertSwarm is driven by a single objective: to constantly compromise the security of our clients through deep detection of blind spots within their cyber defences and technology stacks before real threat actors are able to exploit them.

Continuous offensive security

Our continuous client-focused cyber intelligence gathering, simulated attack, clear vulnerability reporting and follow-up 'Purple Team' education service challenges the status quo of a cyber market that is ripe and in need of modernisation.

Organisations seeking higher degrees of cyber assurance and security confidence than those offered by 'snapshot' penetration testing and red team engagements are increasingly partnering with us. They agree that 'point in time' testing is no longer enough to secure their organisations, and it is through this shared ethos that CovertSwarm challenges everything that is considered 'standard' in today's cyber vendor market. We are not a penetration testing consultancy, red team agency or bug bounty hunter.

Our modern approach

We offer a modern, continuous ethical hacker-led approach to enhancing enterprise security through a blend of constant cyber research and attack that is enhanced through our proximity to our client's teams, knowledge of their business models, and the remedial education that we deliver each time we compromise their defences.

Our founding team and swarm of ethical hackers only include passionate and experienced individuals whose depth of technical and commercial knowledge, diverse hacking skills and real-world cyber battle scars result in a hive of talent that is unique, effective and provides a highly-compelling alternative to clients seeking a modern approach to securing themselves against modern forms of cyber attack.

We are covert by nature, growing through private network referral and cyber community knowledge exchange. Our team members are our greatest resources, and our client's technology estates our most closely-guarded assets.
Don't speak to consultants. Speak to CovertSwarm, today.

13. REFERENCES

01. HTTPS://LABS.F-SECURE.COM/BLOG/SNIFF-THERE-LEAKS-MY-BITLOCKER-KEY/

02. HTTPS://WWW.MOUSER.CO.UK/DATASHEET/2/870/GD25B256D_V1.7_20200612-1668137.PDF

03. HTTPS://WWW.SALEAE.COM/DOWNLOADS/

04. HTTPS://GITHUB.COM/ATUCOM/BITLOCKER-SPI-TOOLKIT/BLOB/KEY-REGEX-FIX/BITLOCKER-KEY-EXTRACTOR/HIGHLEVELANALYZER.PY