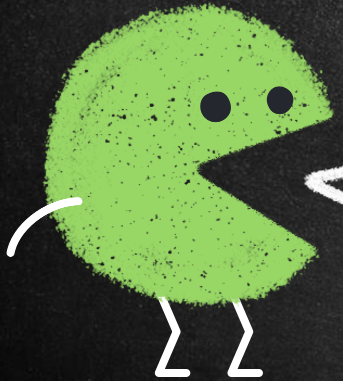
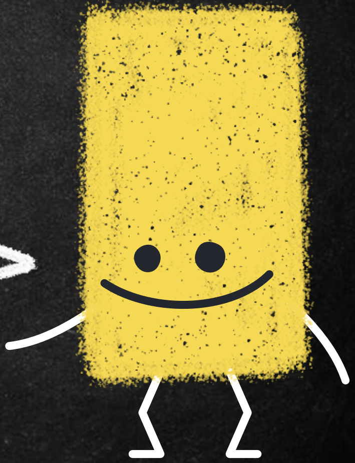
Watching for elmer –

Tips on reviewing documents for Comms Red Flags



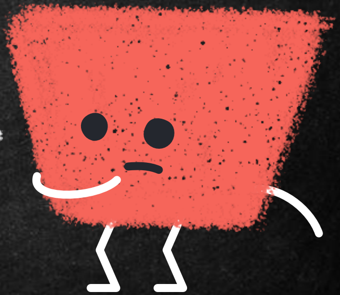


→ What follows is a real-world finding reported to our PSIRT

→ I share this example, as it mirrors many typical academic reports our PSIRT receives

→ These are real things real people said/wanted to say

→ I share insights learned over the years; YOUR mileage may vary



Hi, I'm Crob

Pronunciation: U.S. (K-robe)

Does Stuff

And Things

Risk-ologist, Cat Herder, Pirate, Hat enthusiast, goodly speakerpersonman

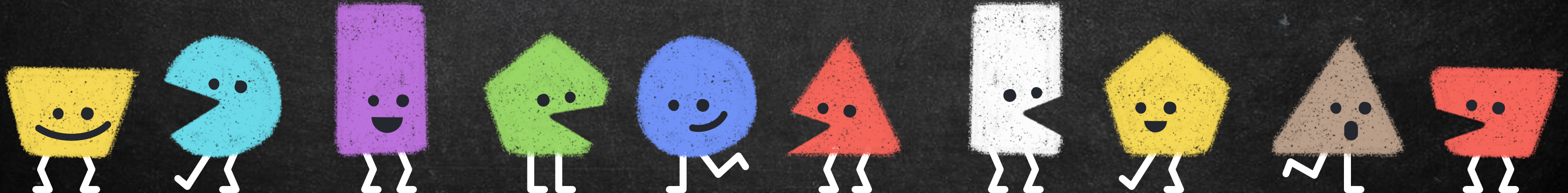
IPAS/IPU Comms

...and other duties as TBD

Hewwo!

This is Elmer FUD

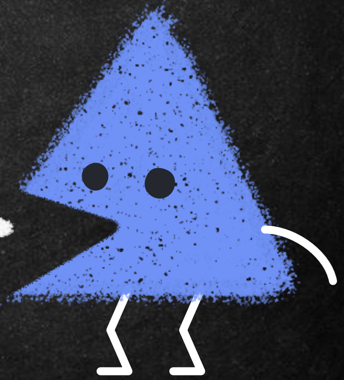
Don't be Elmer



FUD

- → FEAR
- → UNCERTAINTY
- → DOUBT

Part of our job in a PSIRT is to provide clear, calm, objective analysis and advice.



Communicating Security Issues can be Hard

Emotions can be high

Emotions also are not rational

Facts/findings can be unclear

Upon first receiving a researcher’s report both parties are unclear how things will proceed

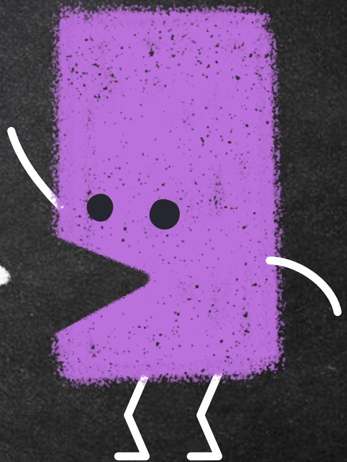
Each party has things to gain/lose

Your first contact/comms with a researcher can set the whole tone of our relationship going forward

“

I must not fear. Fear is the mindkiller that brings total oblivion.

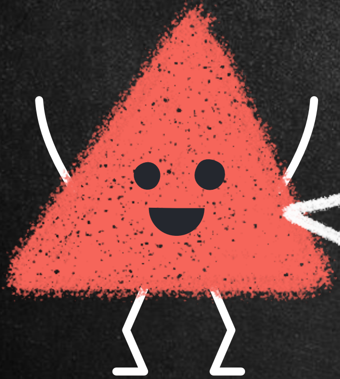
- P. Atredes

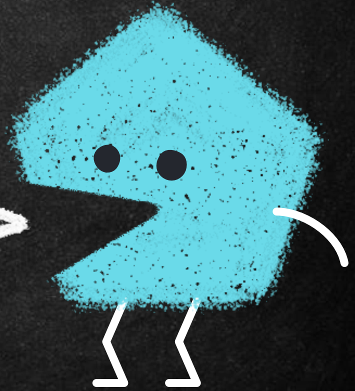


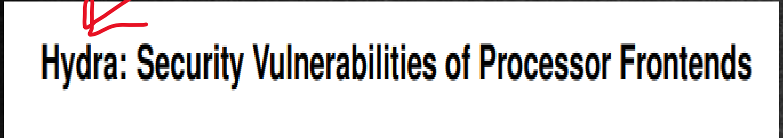
1.

Titles & sections

Let’s start with some easy indicators

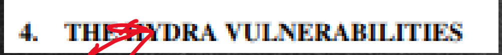






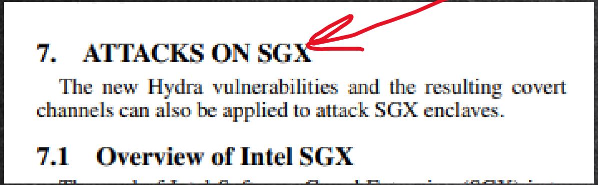
Hydra: Security Vulnerabilities of Processor Frontends

Look for “branding”. Branding will ALWAYS bring more attention to something, regardless of how important is **actually** is



4. THE HYDRA VULNERABILITIES

There it is again!

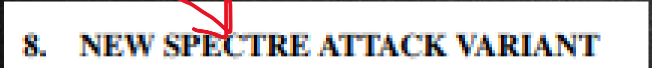


7. ATTACKS ON SGX

The new Hydra vulnerabilities and the resulting covert channels can also be applied to attack SGX enclaves.

7.1 Overview of Intel SGX

Look for concepts/components we REALLY care about



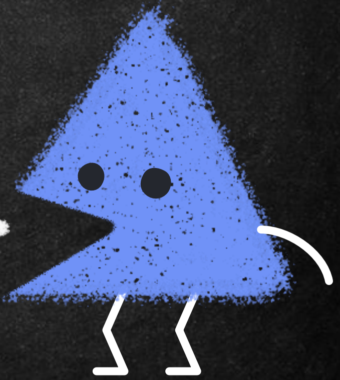
8. NEW SPECTRE ATTACK VARIANT

Look for references to past issues, especially sticky ones for us

A WORD is WORTH A THOUSAND MORE WORDS

The 1st few minutes you have the report, skim through it and look at titles and section headers.

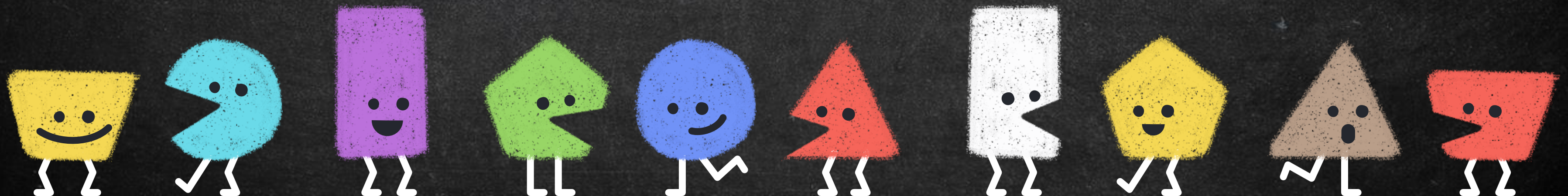
DOES ANYTHING SEEM SCARY or OF CONCERN HERE?

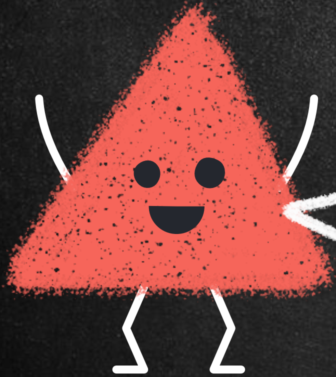


Elmer Alert

Your first look should always be from the perspective of the customer

Customers don't know as much as we do about our tech; scary words and phrases make them anxious

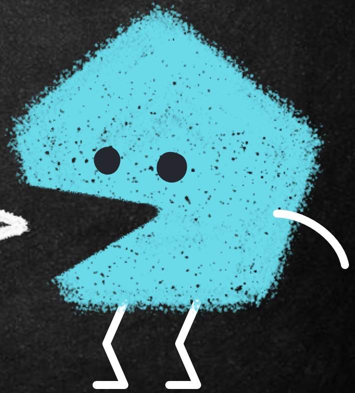




2.

Who is this for?

Why are they telling us about this?



Where they are sharing this is almost as important as what they are sharing

MICRO 2021 Submission

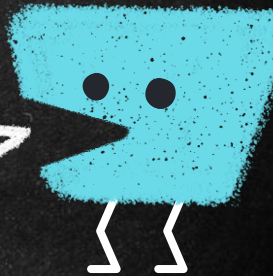
Conferences/Journals

Researcher prestige and fame are factors that can influence how much noise will be made on a paper.

Conferences, media, publications are high-profile venues that will generate more attention

Bounty/Reward

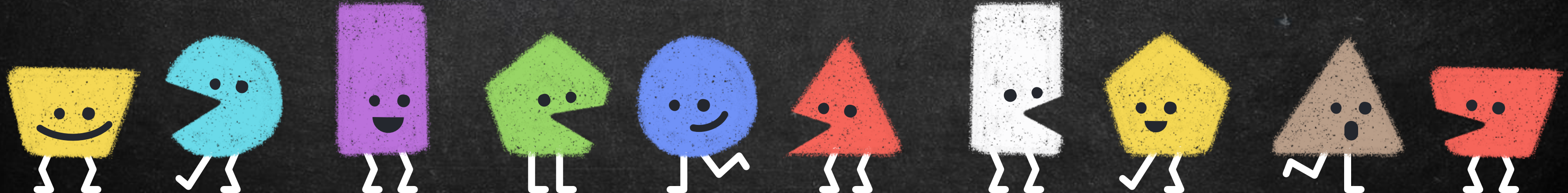
Typically (but not universally) these types of reports will be lower-key since there is some type of conpensation involved

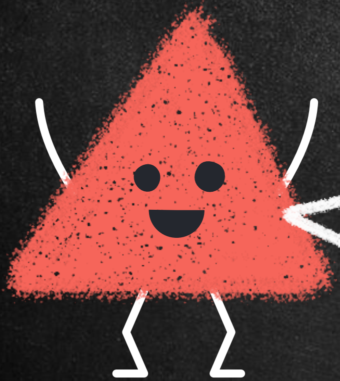


Elmer Alert

Understand how the Finder is going to share this information once it is public

Audience/venue can greatly influence how we need to communicate

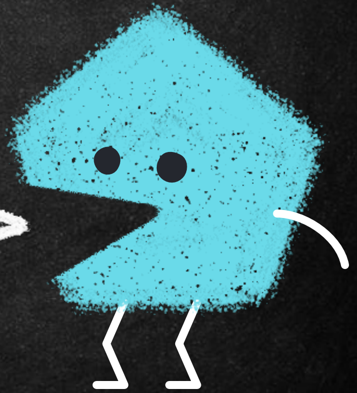


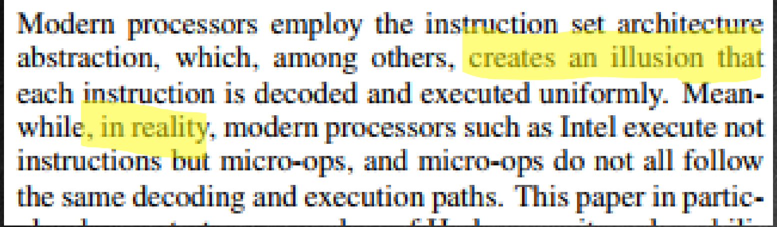


3.

Proactive language

HOW do they talk about their findings?

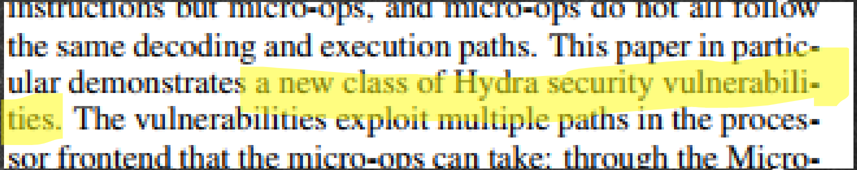




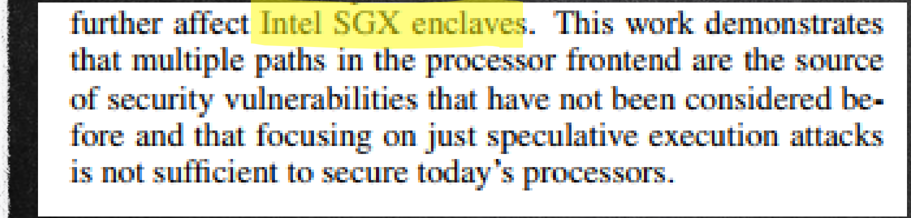
Modern processors employ the instruction set architecture abstraction, which, among others, creates an illusion that each instruction is decoded and executed uniformly. Meanwhile, in reality, modern processors such as Intel execute not instructions but micro-ops, and micro-ops do not all follow the same decoding and execution paths. This paper in partic-

Researchers aren't poets, when flowery words are used, pay attention. Also, these statements are a bit inflammatory, so pay attention

A WHOLE new class of things NEVER seen before? Merits more reading….

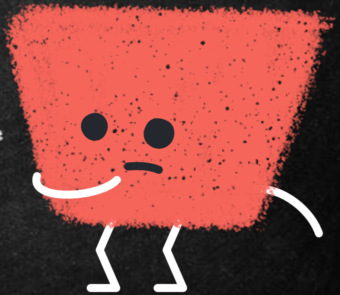


instructions but micro-ops, and micro-ops do not all follow the same decoding and execution paths. This paper in particular demonstrates a new class of Hydra security vulnerabilities. The vulnerabilities exploit multiple paths in the processor frontend that the micro-ops can take: through the Micro-

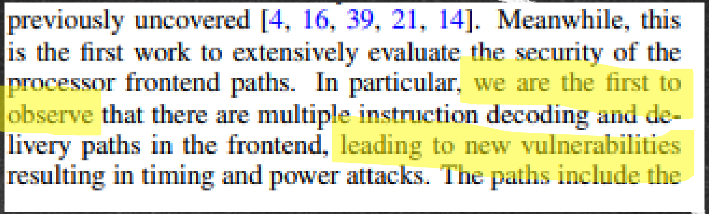


further affect Intel SGX enclaves. This work demonstrates that multiple paths in the processor frontend are the source of security vulnerabilities that have not been considered before and that focusing on just speculative execution attacks is not sufficient to secure today's processors.

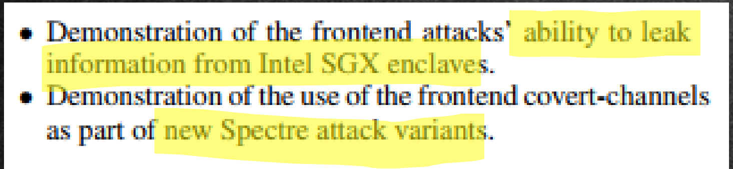
Whenever key security tools or company features are mentioned directly be name, this will draw more attention.



Absolutes “best” “fastest” “first”, “completely”, “always” hint at how they plan might be planning on marketing themselves



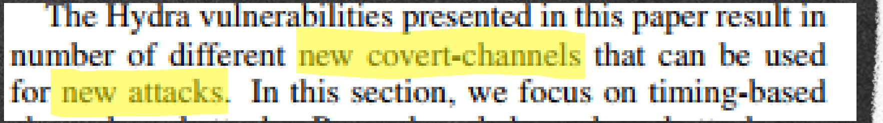
previously uncovered [4, 16, 39, 21, 14]. Meanwhile, this is the first work to extensively evaluate the security of the processor frontend paths. In particular, we are the first to observe that there are multiple instruction decoding and delivery paths in the frontend, leading to new vulnerabilities resulting in timing and power attacks. The paths include the



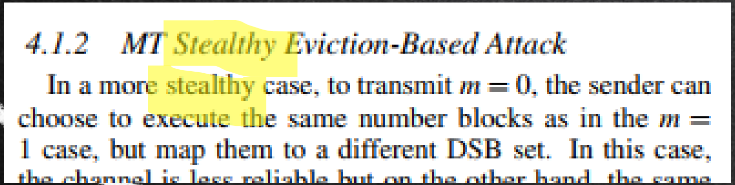
- Demonstration of the frontend attacks' ability to leak information from Intel SGX enclaves.
- Demonstration of the use of the frontend covert-channels as part of new Spectre attack variants.

Again, brand-name stuff to pay attention to

Being a pioneer brings glory for the ages.



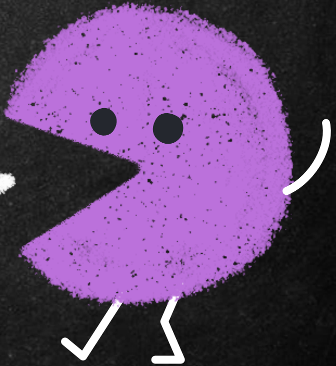
The Hydra vulnerabilities presented in this paper result in number of different new covert-channels that can be used for new attacks. In this section, we focus on timing-based

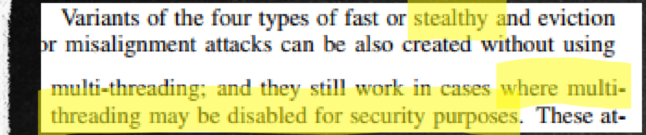


4.1.2 MT Stealthy Eviction-Based Attack

In a more stealthy case, to transmit $m = 0$, the sender can choose to execute the same number blocks as in the $m = 1$ case, but map them to a different DSB set. In this case, the channel is less reliable but on the other hand, the same

Stealth is cool for a plane or a ninja, but as an adjective for research clues us in on their motives/perspectives

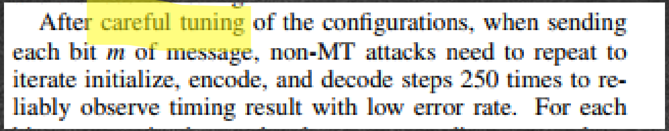




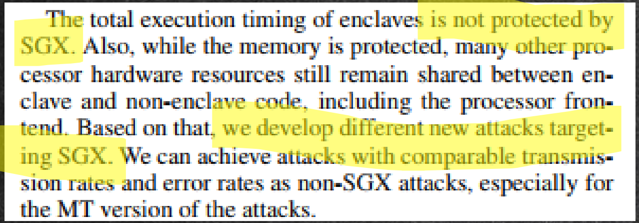
Variants of the four types of fast or stealthy and eviction or misalignment attacks can be also created without using multi-threading; and they still work in cases where multi-threading may be disabled for security purposes. These at-

Stealth again, but here they speak to their attack working even with security features in place. This is a HUGE red flag!!

Anytime a scientist/researcher/hacker uses an adjective, pay attention



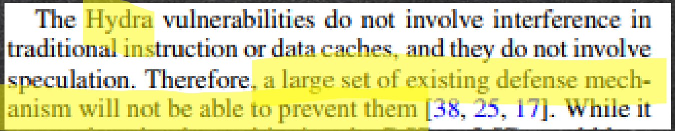
After careful tuning of the configurations, when sending each bit m of message, non-MT attacks need to repeat to iterate initialize, encode, and decode steps 250 times to reliably observe timing result with low error rate. For each



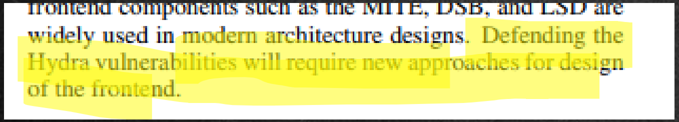
The total execution timing of enclaves is not protected by SGX. Also, while the memory is protected, many other processor hardware resources still remain shared between enclave and non-enclave code, including the processor frontend. Based on that, we develop different new attacks targeting SGX. We can achieve attacks with comparable transmission rates and error rates as non-SGX attacks, especially for the MT version of the attacks.

Again, our security control has been beat! (or so they claim) Also, this is all "new"

Dumb brand-name shows they plan on making noise about this to show how smart they are. Also, our defenses are useless against their kung fu. That's a BOLD claim.

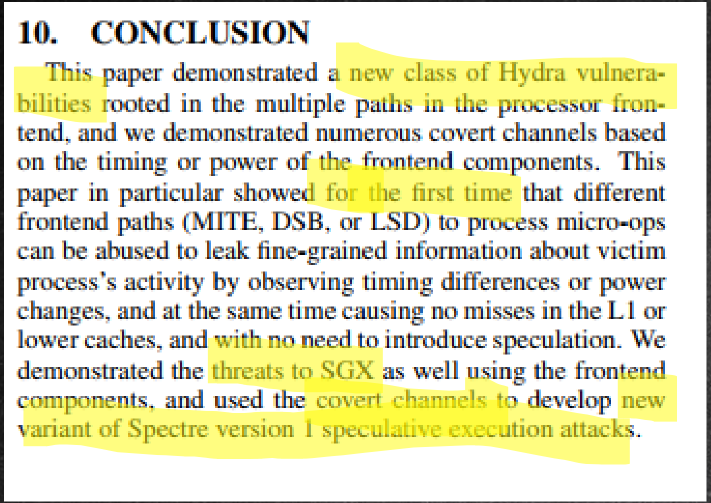


The Hydra vulnerabilities do not involve interference in traditional instruction or data caches, and they do not involve speculation. Therefore, a large set of existing defense mechanism will not be able to prevent them [38, 25, 17]. While it



frontend components such as the MITE, DSB, and LSD are widely used in modern architecture designs. Defending the Hydra vulnerabilities will require new approaches for design of the frontend.

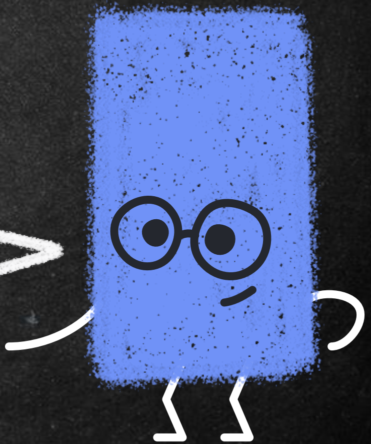
Again, combating their awesome flaw will be nigh-impossible.



10. CONCLUSION

This paper demonstrated a new class of Hydra vulnerabilities rooted in the multiple paths in the processor frontend, and we demonstrated numerous covert channels based on the timing or power of the frontend components. This paper in particular showed for the first time that different frontend paths (MITE, DSB, or LSD) to process micro-ops can be abused to leak fine-grained information about victim process's activity by observing timing differences or power changes, and at the same time causing no misses in the L1 or lower caches, and with no need to introduce speculation. We demonstrated the threats to SGX as well using the frontend components, and used the covert channels to develop new variant of Spectre version 1 speculative execution attacks.

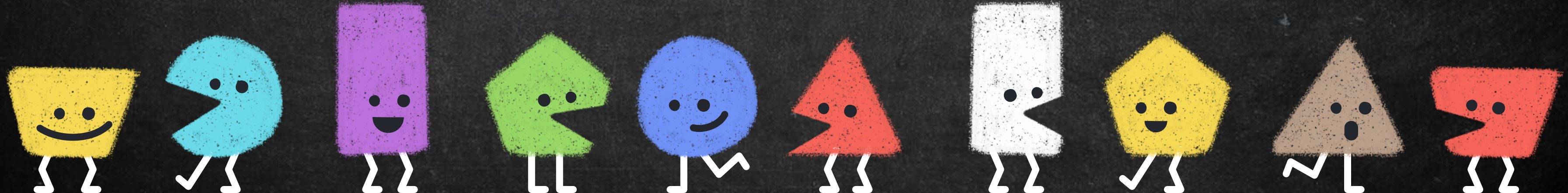
The conclusion restates everything we've seen through out the paper, and again, could be used for a quick "pulse check" of what the researchers are about and a bit about what they intend.

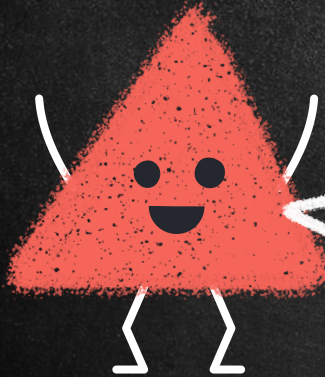


Elmer Alert

Be on the look out for "exciting" words

Customers and the Media might also find them more exciting than they really are

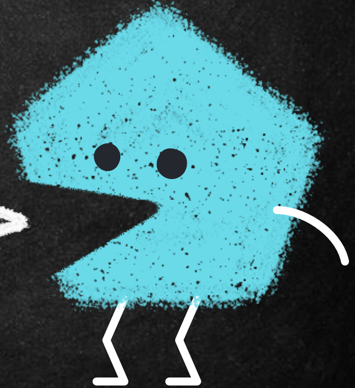




4.

HISTORY

WHO are these people?



Have you ever talked to these folks before?

How did it go?

If it went well….can you replicate that experience again?

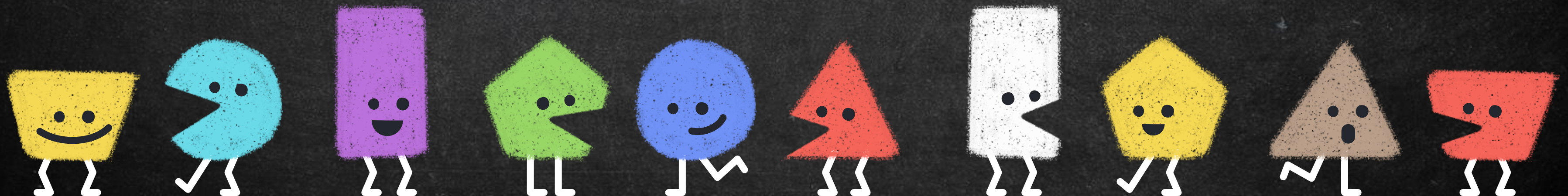
If it went poorly…what might have been done to salvage that interaction?

Has the Finder provided any clues in how they plan on disclosing this issue?

Imaged by Heritage Auctions, HA.com

If not, have you talked to people *like* these reporters?

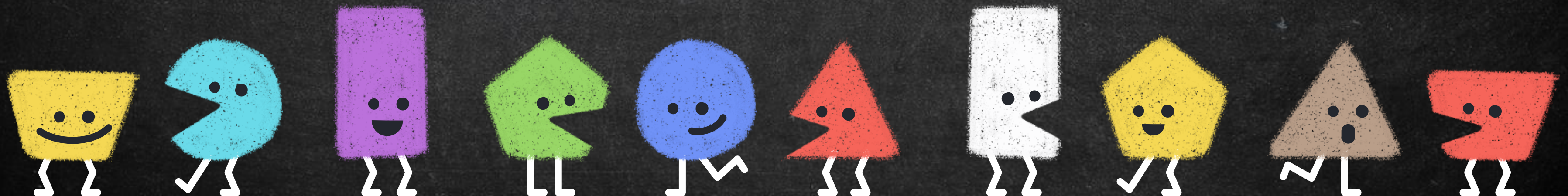
Do you have a profile that documents how that reporter’s persona is motivated?
How might they react?
How do they view CVD?
Have they “marketed” findings before?



Elmer Alert

Keep a profile on researchers so you track how they behave

If they did something before, odds are good they’ll do the same thing again

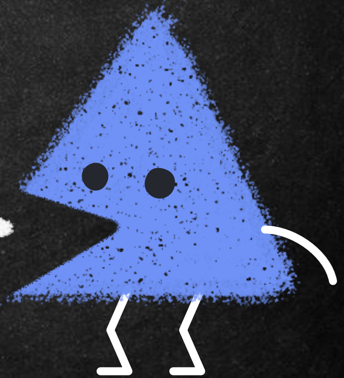


Red Flag Recap

- Do a quick scan of a report looking for exciting words
- Watch for claims of “completely circumventing security”
- Understand who is reporting this to you and how they might react going forward

This can help us prepare for any unexpected “oops” while more in-depth technical analysis proceeds

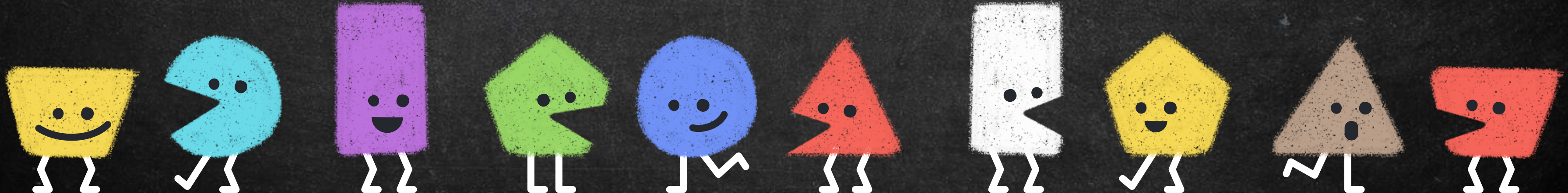
Celebrity/branded things will ALWAYS draw more attention than the “boring” ones.

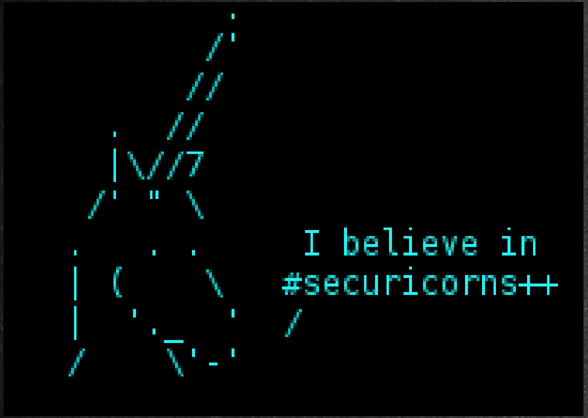


Elmer Alert

Regardless of the technical merits of a report, certain words, phrases, and actions can have wide public consequences

View the report as if you were a layperson first to see what might excite them





✉ CRob_at_Intel_dot_com

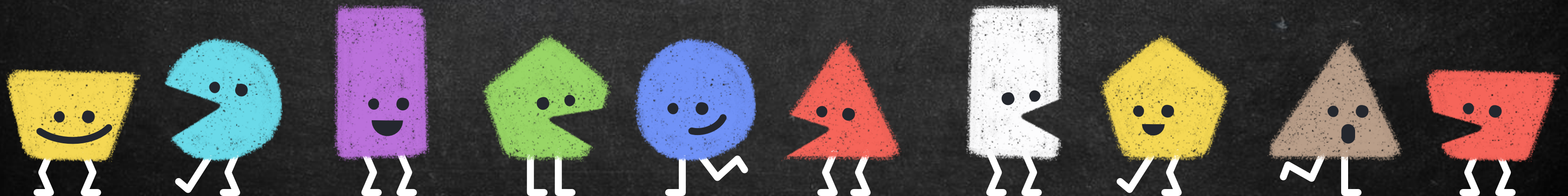
@SecurityCRob

@SecurityCRob@infosec.exchange

https://github.com/SecurityCRob

The Security Unhappy Hour,
Chips & Salsa

https://www.linkedin.com/in/darthcrob/



THIS IS THE WAY
I HAVE SPOKEN
MEMEFUL.COM