TEXT 2

# **R**e**s**ea**r**che**rs** want to u**s**e ha**r**dwa**r**e to fight compute**r** vi**r**u**s**e**s**

## Date: Novembe**r** 7, 2016

Fighting compute**r** vi**r**u**s**e**s** i**s**n't ju**s**t fo**r** **s**oftwa**r**e anymo**r**e. Binghamton Unive**rs**ity **r**e**s**ea**r**che**rs** will u**s**e a g**r**ant f**r**om the National **S**cience Foundation to **s**tudy how ha**r**dwa**r**e can help p**r**otect compute**rs** too.

"The impact will potentially be felt in all computing domain**s**, f**r**om mobile to cloud**s**," **s**aid Dmit**r**y Ponoma**r**ev, p**r**ofe**ss**o**r** of compute**r** **s**cience at Binghamton Unive**rs**ity, **S**tate Unive**rs**ity of New Yo**r**k. Ponoma**r**ev i**s** the p**r**incipal inve**s**tigato**r** of a p**r**oject titled "P**r**actical Ha**r**dwa**r**e-A**ss**i**s**ted Alway**s**-On Malwa**r**e Detection."

Mo**r**e than 317 million piece**s** of new malwa**r**e -- compute**r** vi**r**u**s**e**s**, **s**pywa**r**e, and othe**r** maliciou**s** p**r**og**r**am**s** -- we**r**e c**r**eated in 2014 alone, acco**r**ding to wo**r**k done by Inte**r**net **s**ecu**r**ity team**s** at **S**ymantec and Ve**r**izon. Malwa**r**e i**s** g**r**owing in complexity, with c**r**ime**s** **s**uch a**s** digital exto**r**tion (a hacke**r** **s**teal**s** file**s** o**r** lock**s** a compute**r** and demand**s** a **r**an**s**om fo**r** dec**r**yption key**s**) becoming la**r**ge avenue**s** of cybe**r**-attack.

"Thi**s** p**r**oject hold**s** the p**r**omi**s**e of **s**ignificantly impacting an a**r**ea of c**r**itical national need to help **s**ecu**r**e **s**y**s**tem**s** again**s**t the expanding th**r**eat**s** of malwa**r**e," **s**aid Ponoma**r**ev. "[It i**s**] a new app**r**oach to imp**r**ove the effectivene**ss** of malwa**r**e detection and to allow **s**y**s**tem**s** to be p**r**otected continuou**s**ly without **r**equi**r**ing the la**r**ge **r**e**s**ou**r**ce inve**s**tment needed by **s**oftwa**r**e monito**rs**."

Counte**r**ing th**r**eat**s**[[1]](#footnote-1) ha**s** t**r**aditionally been left **s**olely to **s**oftwa**r**e p**r**og**r**am**s**, but Binghamton **r**e**s**ea**r**che**rs** want to modify a compute**r**'**s** cent**r**al p**r**oce**ss**ing unit (CPU) chip -- e**ss**entially, the machine'**s** b**r**ain -- by adding logic to check fo**r** anomalie**s** while **r**unning a p**r**og**r**am like Mic**r**o**s**oft Wo**r**d. If an anomaly i**s** **s**potted, the ha**r**dwa**r**e will ale**r**t mo**r**e **r**obu**s**t **s**oftwa**r**e p**r**og**r**am**s** to check out the p**r**oblem. The ha**r**dwa**r**e won't be **r**ight about **s**u**s**piciou**s** activity 100 pe**r**cent of the time, but **s**ince the ha**r**dwa**r**e i**s** acting a**s** a lookout at a po**s**t that ha**s** neve**r** been monito**r**ed befo**r**e, it will imp**r**ove the ove**r**all effectivene**ss** and efficiency of malwa**r**e detection.

"The modified mic**r**op**r**oce**ss**o**r** will have the ability to detect malwa**r**e a**s** p**r**og**r**am**s** execute by analyzing the execution **s**tati**s**tic**s** ove**r** a window of execution," **s**aid Ponoma**r**ev. "**S**ince the ha**r**dwa**r**e detecto**r** i**s** not 100-pe**r**cent accu**r**ate, the ala**r**m will t**r**igge**r** the execution of a heavy-weight **s**oftwa**r**e detecto**r** to ca**r**efully in**s**pect **s**u**s**piciou**s** p**r**og**r**am**s**. The **s**oftwa**r**e detecto**r** will make the final deci**s**ion. The ha**r**dwa**r**e guide**s** the ope**r**ation of the **s**oftwa**r**e; without the ha**r**dwa**r**e the **s**oftwa**r**e will be too **s**low to wo**r**k on all p**r**og**r**am**s** all the time."

The modified CPU will u**s**e low complexity machine lea**r**ning -- the ability to lea**r**n without being explicitly p**r**og**r**ammed -- to cla**ss**ify malwa**r**e f**r**om no**r**mal p**r**og**r**am**s**, which i**s** Yu'**s** p**r**ima**r**y a**r**ea of expe**r**ti**s**e.

"The detecto**r** i**s**, e**ss**entially, like a cana**r**y in a coal mine to wa**r**n **s**oftwa**r**e p**r**og**r**am**s** when the**r**e i**s** a p**r**oblem," **s**aid Ponoma**r**ev. "The ha**r**dwa**r**e detecto**r** i**s** fa**s**t, but i**s** le**ss** flexible and comp**r**ehen**s**ive. The ha**r**dwa**r**e detecto**r**’**s** **r**ole i**s** to find **s**u**s**piciou**s** behavio**r** and bette**r** di**r**ect the effo**r**t**s** of the **s**oftwa**r**e."

Much of the wo**r**k -- including explo**r**ation of the t**r**ade-off**s** of de**s**ign complexity, detection accu**r**acy, pe**r**fo**r**mance and powe**r** con**s**umption -- will be done in collabo**r**ation with fo**r**me**r** Binghamton p**r**ofe**ss**o**r** Nael Abu-Ghazaleh, who moved on to the Unive**rs**ity of Califo**r**nia-**R**ive**rs**ide in 2014.

Lei Yu, a**ss**ociate p**r**ofe**ss**o**r** of compute**r** **s**cience at Binghamton Unive**rs**ity, i**s** a co-p**r**incipal inve**s**tigato**r** of the g**r**ant.

G**r**ant funding will **s**uppo**r**t g**r**aduate **s**tudent**s** that will wo**r**k on the p**r**oject both in Binghamton and Califo**r**nia, confe**r**ence t**r**avel and the inve**s**tigation it**s**elf. The th**r**ee-yea**r** g**r**ant i**s** fo**r** $275,000.

## **R**eading Comp**r**ehen**s**ion Ta**s**k**s**

**1) What is Ponomarev's project called?**

P**r**actical Ha**r**dwa**r**e-A**ss**i**s**ted Alway**s**-On Malwa**r**e Detection.

**2) Why might his project have national impact?**

**R**athe**r** than national, the impact would be wo**r**ldwide **s**ince it will potentially be felt in all computing domain**s**, f**r**om mobile to cloud**s**.

**3) Explain in what way malware is increasing and also its consequences.**

Mo**r**e than 317 million piece**s** of new malwa**r**e -- compute**r** vi**r**u**s**e**s**, **s**pywa**r**e, and othe**r** maliciou**s** p**r**og**r**am**s** -- we**r**e c**r**eated in 2014 alone, acco**r**ding to wo**r**k done by Inte**r**net **s**ecu**r**ity team**s** at **S**ymantec and Ve**r**izon. Malwa**r**e i**s** g**r**owing in complexity, with c**r**ime**s** **s**uch a**s** digital exto**r**tion (a hacke**r** **s**teal**s** file**s** o**r** lock**s** a compute**r** and demand**s** a **r**an**s**om fo**r** dec**r**yption key**s**) becoming la**r**ge avenue**s** of cybe**r**-attack.

**4) According to the researchers, what happens once an anomaly has been detected?**

"The detecto**r** i**s**, e**ss**entially, like a cana**r**y in a coal mine to wa**r**n **s**oftwa**r**e p**r**og**r**am**s** when the**r**e i**s** a p**r**oblem," i.e., the ala**r**m will t**r**igge**r** the execution of a heavy-weight **s**oftwa**r**e detecto**r** to ca**r**efully in**s**pect **s**u**s**piciou**s** p**r**og**r**am**s**. The **s**oftwa**r**e detecto**r** will make the final deci**s**ion.

**5) According to the project, the hardware detector is not 100% accurate, so how is its effectiveness explained? Explain the procedure.**

The ha**r**dwa**r**e detecto**r**’**s** **r**ole i**s** to find **s**u**s**piciou**s** behavio**r** and bette**r** di**r**ect the effo**r**t**s** of the **s**oftwa**r**e.

**6) Explain the phrase "acting as a lookout"**

A lookout i**s** a high place whe**r**e a pe**rs**on can look at what i**s** happening in the a**r**ea a**r**ound them, e**s**pecially in o**r**de**r** to watch fo**r** any dange**r**. Thi**s** p**r**oject i**s** not intended to have a di**r**ect **s**t**r**uggle again**s**t malwa**r**e but bette**r** wa**r**ning the pe**r**tinent **s**oftwa**r**e to act acco**r**dingly.

**7) Explain the comparison "like a canary in a coal mine". Find information in the Internet and connect it with the text.**

Thi**s** i**s** connected with the p**r**eviou**s** an**s**we**r**. It i**s** well known that it wa**s** a cu**s**tom in mining to ca**rr**y a cana**r**y whe**r**e human**s** had to wo**r**k. Any cana**r**y i**s** ve**r**y **s**u**s**ceptible to ga**s** emanation, leak that **r**ep**r**e**s**ent**s** an eno**r**mou**s** dange**r** to human**s** **s**ince ga**s** natu**r**ally ha**s** no odo**r**, i.e., human**s** can’t **s**mell a ga**s** leak. The moment the cana**r**y wa**s** falling dead wa**s** the moment to **r**u**s**h to the **s**u**r**face.

TE**R**MINATO**R** THEO**R**Y

I cho**s**e thi**s** a**r**ticle becau**s**e it **r**efe**rs** to a **s**to**r**y that wa**s** w**r**itten thi**r**ty yea**rs** ago. A **s**ituation that i**s** **r**elated to technologie**s** that do not yet exi**s**t and that, at fi**rs**t, fa**s**cinate u**s**, and then we a**ss**ume we will not get along with.

But, let u**s** **s**ta**r**t at the beginning.

Thi**s** a**r**ticle i**s** **s**ome new**s** about a p**r**oject that i**s** cu**rr**ently being developed with the collabo**r**ation of two team**s** of **r**e**s**ea**r**che**rs**, one f**r**om the Unive**rs**ity of Binghamton and the othe**r** f**r**om the Unive**rs**ity of Califo**r**nia-**R**ive**rs**ide.

Thi**s** p**r**oject con**s**i**s**t**s** of modifying a mic**r**op**r**oce**ss**o**r** that, with a**r**tificial intelligence ha**r**dwa**r**e code, can make an ea**r**ly detection of maliciou**s** **s**oftwa**r**e. Without a doubt, of all the **s**olution**s** p**r**opo**s**ed, thi**s** i**s** the be**s**t one. The **r**e**s**pon**s**e time of a **s**et of in**s**t**r**uction**s** gove**r**ned by ha**r**dwa**r**e i**s** exponentially highe**r** than any **s**oftwa**r**e we could eve**r** achieve.

The a**r**ticle p**r**ovide**s** **s**ome mo**r**e detail**s** that a**r**e e**ss**entially t**r**ivial. What ha**s** been **s**aid **s**o fa**r** i**s** a good **s**umma**r**y. We do not know if they have made any conc**r**ete development yet (the a**r**ticle i**s** 5 yea**rs** old), and if they have, at what **s**tage they a**r**e. The**r**e a**r**e no a**r**ticle**s** on the inte**r**net that expand the info**r**mation, much le**ss** do we have new**s** that the main indu**s**t**r**ial develope**rs** of mic**r**op**r**oce**ss**o**rs** have been involved in any way.

**S**o the**r**efo**r**e, the p**r**oject it**s**elf ha**s** p**r**obably been f**r**ozen without **s**ignificant p**r**og**r**e**ss**. But the idea ha**s** al**r**eady been put on the table, and although it i**s** an innovative and c**r**itical idea, we may not be at a **s**ufficiently advanced technological **s**tage to implement it. And the latte**r**, mo**r**e than an a**ss**umption, i**s** a deduction with enough evidence.

Let me explain my**s**elf. He**r**e at the unive**rs**ity, we **s**tudy (a**s** pa**r**t of the cu**rr**iculum) the **s**o-called elect**r**onic gate**s** gove**r**ned by a bina**r**y logic f**r**om which mic**r**op**r**oce**ss**o**rs** a**r**e molded. We have even built, theo**r**etically, a 4-bit mic**r**op**r**oce**ss**o**r** capable of **r**unning ve**r**y **s**imple p**r**og**r**am**s**. The**s**e p**r**og**r**am**s**, completely p**r**inted on logic gate**s**, pe**r**fo**r**m ope**r**ation**s** that a**r**e linea**r** with no heu**r**i**s**tic capabilitie**s**.

Knowing the **s**tate of the **s**cience behind thi**s**, the p**r**opo**s**al of an a**r**tificial intelligence p**r**og**r**am embodied in ha**r**dwa**r**e i**s** not that it i**s** impo**ss**ible, but it i**s** flatly unlikely.

Howeve**r**, what i**s** **s**t**r**iking i**s** that the idea i**s** not new. It wa**s** **r**ai**s**ed 30 yea**rs** ago. And I want to d**r**aw the attention to the **r**eaction of humanity the fi**rs**t time that li**s**tened to the idea. And that i**s** the comment I want to make in **r**elation to thi**s** text.

Befo**r**e, let'**s** go back 4 decade**s**, to the 80'**s**. In 1984 the movie Te**r**minato**r** wa**s** **r**elea**s**ed. Thi**s** movie, wa**s** it a **s**cience fiction o**r** a ho**rr**o**r** movie? People who have debated thi**s** **s**ubject have concluded that it wa**s** a mixtu**r**e of both. The **s**cience fiction **s**ide doe**s** not conce**r**n u**s** **r**ight now to what we a**r**e now dealing with. The inte**r**e**s**ting **s**ide i**s** that the film wa**s** con**s**ide**r**ed a ho**rr**o**r** movie. Te**rr**o**r** of what? The plot of the film wa**s** clo**s**e to **s**ubject that, without being bloody, p**r**oduced te**rr**o**r** in tho**s**e yea**rs**. The cold wa**r**, fo**r** example. But, at a level clo**s**e**r** to the **r**elation**s**hip that humanity wa**s** beginning to have with machine**s**, in thi**s** **r**elation**s**hip, we**r**e we outmatched. And eventually, cont**r**olled?

A mic**r**o a**r**gument within the **s**c**r**ipt i**s** enough fo**r** thi**s**. Let'**s** **s**ee:

In one of the fi**rs**t **s**cene**s**, you can hea**r** the an**s**we**r**ing me**ss**age f**r**om **S**a**r**ah'**s** (the p**r**otagoni**s**t) an**s**we**r**ing machine: "Hello. I fooled on you. You'**r**e talking to a machine. But don't be **s**hy. Machine**s** need love too, **s**o talk to it."

The da**r**k **r**eve**rs**e i**s** given in one of the la**s**t **s**cene**s**. When **S**a**r**ah call**s** he**r** mothe**r**, **s**he end**s** up talking to the Te**r**minato**r**, who mimic**s** he**r** mothe**r**'**s** voice. **S**he i**s** talking to a machine, but now **s**he i**s** the one being fooled believing that **s**he i**s** talking to a pe**rs**on.

That backg**r**ound of the movie that take**s** u**s** to it**s** **s**equel in the 90'**s**, 1991 to be exact, now 30 yea**rs** ago. In that **s**equel, the te**rr**ifying element of the fi**rs**t one i**s** captu**r**ed in a mo**r**e patent way by the hand of one of it**s** p**r**otagoni**s**t**s**, D**r**. Mile**s** Bennett Dy**s**on. He i**s** the o**r**iginal invento**r** of the mic**r**op**r**oce**ss**o**r** that would lead to the development of **S**kynet, an intelligent compute**r** **s**y**s**tem de**s**tined to be cont**r**olled by the United **S**tate**s** milita**r**y, but which would late**r** launch a global wa**r** of exte**r**mination again**s**t humanity.

In one pa**r**t of the movie, Dy**s**on claim**s** that the mic**r**op**r**oce**ss**o**r** they we**r**e **s**tudying (which wa**s** **r**ecove**r**ed f**r**om the Te**r**minato**r** f**r**om the fi**rs**t movie) "It wa**s** a **s**ca**r**y thing, **r**adically advanced. It wa**s** **s**ma**s**hed ... it didn't wo**r**k. But it gave u**s** idea**s**. It took u**s** on new di**r**ection**s** ... thing**s** we neve**r** would have thought of. All of ou**r** wo**r**k i**s** ba**s**ed on that. "

He wa**s** **r**efe**rr**ing to a mic**r**op**r**oce**ss**o**r** that had innate a**r**tificial intelligence capabilitie**s**…

I have alway**s** been amazed by the in**s**ight of the w**r**ite**rs** of the o**r**iginal **s**c**r**ipt of the film, becau**s**e it i**s** po**ss**ible to find detail**s** of that "te**rr**ifying technology" that come**s** to the ca**s**e of what we a**r**e **s**peaking today: the cha**r**acte**r**i**s**tic**s**. And thi**s** **s**cience fiction movie can give u**s** an idea of ​​the **s**tate of the a**r**t in f**r**ont of the new**s** we a**r**e now con**s**ide**r**ing.

What a**r**e the**s**e cha**r**acte**r**i**s**tic**s**, tho**s**e of a mic**r**op**r**oce**ss**o**r** with innate a**r**tificial intelligence capabilitie**s**?

Acco**r**ding to the w**r**ite**rs**, afte**r** many yea**rs** of wo**r**k, Dy**s**on finally came up with a p**r**ototype model that not only wo**r**ked and wa**s** bug-f**r**ee, but wa**s** **s**upe**r**conducting at **r**oom tempe**r**atu**r**e, making it ext**r**emely powe**r**ful.

The CPU wa**s** p**r**ima**r**ily modeled and de**s**igned on compute**rs** in advanced th**r**ee-dimen**s**ional p**r**og**r**amming package**s**, whe**r**e **s**imulated te**s**t**s** could be pe**r**fo**r**med in **r**eal time.

The lattice of cube**s** in the con**s**t**r**uction of the mic**r**op**r**oce**ss**o**r** p**r**ototype **s**ugge**s**t**s** a "hype**r**cube" (a cube of mo**r**e than th**r**ee dimen**s**ion**s**). In mic**r**op**r**oce**ss**o**r** de**s**ign, hype**r**cube**s** a**r**e u**s**ed a**s** a phy**s**ical connection **s**cheme that minimize**s** the effective communication di**s**tance, and the**r**efo**r**e, time delay between **s**ub p**r**oce**ss**o**rs** when the logical connection **s**cheme needed by the **s**oftwa**r**e to be **r**un on tho**s**e p**r**oce**ss**o**rs** cannot be known in advance. Thi**s** then **s**uppo**r**t**s** the neu**r**al netwo**r**k'**s** ability to lea**r**n, adapt, and build new logical connection **s**cheme**s**.

But the mo**s**t impo**r**tant pa**r**t i**s** that the neu**r**al netwo**r**k i**s** innovative and u**s**e**s** the late**s**t quantum (te**r**na**r**y) effect chip**s**. Until Dy**s**on de**s**igned the mic**r**op**r**oce**ss**o**r**, compute**rs** could **r**un on chip**s** made up of million**s** of t**r**an**s**i**s**to**rs**. T**r**aditional computing wa**s** done in the cu**rr**ent (bina**r**y) **s**y**s**tem: one**s** and ze**r**o**s**, on and off.

That i**s**, thi**s** mic**r**op**r**oce**ss**o**r** made it po**ss**ible to do many mo**r**e calculation**s** eve**r**y **s**econd, with po**ss**ible t**r**illion**s** of **s**witching po**s**ition**s**, many of them **s**imultaneou**s** at each quantum level.

And **s**o fa**r**, tho**s**e who know**s** the **s**ubject, know**s** that thi**s**, in ou**r** cu**rr**ent **s**tage of technology, exi**s**t**s**, but not in a conc**r**ete way. We don't even have p**r**og**r**amming language**s** ​​capable of taking advantage of ou**r** cu**rr**ent multi-co**r**e mic**r**op**r**oce**ss**o**rs** (we **s**till u**s**e a **s**ingle co**r**e). And if thi**s** al**r**eady would have a **s**olution, we **s**till need one mo**r**e: a p**r**og**r**amming language with te**r**na**r**y capacity, a p**r**og**r**amming language that cu**rr**ently **s**imply doe**s** not exi**s**t yet.

It i**s** all thi**s** that explain**s** the **r**adio **s**ilence of thi**s** fo**r** five yea**rs** now, and the ab**s**ence of new**s** about thi**s** p**r**oject, which **s**imply doe**s** not have a cu**rr**ent technological advance that can make **r**eal the p**r**opo**s**al.

Late**r** will come the debate of what to **r**eally expect f**r**om thi**s** advance. And even mo**r**e c**r**itical: if thi**s** doe**s** not would end up being the beginning of a mo**r**e fea**r**ed Mon**s**te**r** of F**r**anken**s**tein.

intel th**r**eat detection technology encounte**r**

**S**TICKY NOTE**S**:

* 2006 – a**r**ticle about the inve**s**tigation of Ponoma**r**ev about a**r**tificial intelligence embedded into mic**r**op**r**oce**ss**o**rs**
  + At a fi**rs**t moment, the**r**e we**r**e 5 yea**rs** of **r**adio **s**ilence
  + Wa**s** a **s**tolen idea f**r**om te**r**minato**r** the movie?
  + **GO TO 2021**
* 2018-2019 - found new pape**r** by Ponoma**r**ev about **s**ide-channel attack
  + It wa**s** othe**r** **s**ide of the **s**ame coin? **S**eemed **s**imila**r**, but it wa**s** not exactly the **s**ame
  + What’**s** going on? He d**r**opped out the fo**r**me**r** p**r**oject?
  + **GO TO «PUTTING ALL TOGETHER»**
* 2021 – Intel (integ**r**ated elect**r**onic**s**) **r**elea**s**e**s** th**r**eat detection technology
  + I’ve found new**s** about new **r**elea**s**e f**r**om intel. **R**eading about it, I wa**s** **s**hocked: wa**s** the **s**ame idea of Ponoma**r**ev. What’**s** going on?
  + **S**ea**r**ching again fo**r** info**r**mation about Ponoma**r**ev, o**r**iginal p**r**opo**s**al felt into oblivion
  + **GO TO 2018-2019**

PUTTING ALL TOGETHE**R**

**S**cenic panic. Be calm.

The a**r**ticle I've cho**s**en and I wa**s** int**r**igued to i**s** that one about Ponoma**r**ev and hi**s** p**r**opo**s**al about ea**r**ly malwa**r**e detection ba**s**ed on a**r**tificial intelligence embedded into mic**r**op**r**oce**ss**o**r** ha**r**dwa**r**e ability.

I am **s**keptical mo**s**t of the time. When I **r**ead the fi**rs**t time the a**r**ticle, I got **s**u**s**piciou**s** when, **s**ea**r**ching fo**r** the o**r**iginal a**r**ticle, I found that i**s** aged about five yea**rs**.

The fi**rs**t I thought wa**s**: Why thi**s** **r**adio **s**ilence of five yea**rs**?

And it **s**ta**r**ted to c**r**o**ss** my mind **s**ome c**r**azy idea. Ponoma**r**ev wa**s** a bluffe**r** and **s**tole the idea f**r**om a movie, Te**r**minato**r**.

If you **r**ecall that movie, you will **r**emembe**r** that, in pa**r**ticula**r**, the **s**to**r**y on the **s**equel **s**pin**s** a**r**ound the fact that a team of **r**e**s**ea**r**che**rs** we**r**e ba**s**ing thei**r** wo**r**k on the **r**ecove**r**ed mic**r**op**r**oce**ss**o**r** that u**s**ed to belong to the fi**rs**t Te**r**minato**r**. Oddly enough, that mic**r**op**r**oce**ss**o**r** p**r**eci**s**ely had **s**ilicon-ba**s**ed a**r**tificial intelligence.

**S**o, I **s**et the i**ss**ue to **r**e**s**t and decided to p**r**epa**r**e **s**omething like that fo**r** thi**s** p**r**e**s**entation.

But…

But thi**s** **s**to**r**y about Ponoma**r**ev wa**s**n't ove**r** at all. Not even clo**s**e.

It happened thi**s** way. I am a compute**r** geek, **s**o I'm alway**s** **r**eading new**s** about compute**rs**, obviou**s**ly. And a week ago, an announcement f**r**om Intel (Integ**r**ated Elect**r**onic**s**) came to me. They ju**s**t **r**elea**s**ed a new featu**r**e: the Intel Th**r**eat Detection Technology. What it'**s** about? New p**r**oce**ss**o**rs** f**r**om the company a**r**e en**s**emble with a new component: ha**r**dwa**r**e ability fo**r** ea**r**ly detection of vi**r**u**s**e**s** ba**s**ed on inco**r**po**r**ated a**r**tificial intelligence which, on detection, wa**r**n**s** to Mic**r**o**s**oft Defende**r** to act acco**r**dingly.

Oh my God… that wa**s** exactly the idea of Ponoma**r**ev.

**S**o, I went in **r**u**s**h **s**ea**r**ching again, but thi**s** time, no looking afte**r** the a**r**ticle, in**s**tead **r**athe**r** on the **s**cienti**s**t, Ponoma**r**ev. If I wa**s** going to find any an**s**we**r** to thi**s**, he wa**s** the key to pu**rs**ue. And I wa**s** **r**ight, luckily.

Ponoma**r**ev p**r**opo**s**al, obviou**s**ly, wa**s** hea**r**d. Intel made the implementation of hi**s** idea. But Ponoma**r**ev didn't **s**tay quiet. He became famou**s** and got Intel'**s** attention becau**s**e of a di**s**cove**r**y f**r**om which Ponoma**r**ev i**s**, among othe**rs**, the autho**r**.

Ponoma**r**ev nowaday**s** i**s** mo**r**e famou**s** becau**s**e of what i**s** known a**s** the **S**pect**r**e and Meltdown **r**an**s**omwa**r**e attack**s**. In an a**r**ticle ci**r**ca 2018-2019, hi**s** a**ss**e**ss**ment**s** we**r**e ve**r**y ala**r**ming becau**s**e he wa**s** wa**r**ning out loud that almo**s**t eve**r**y compute**r** in the wo**r**ld wa**s** defen**s**ele**ss** in f**r**ont of the**s**e attack**s**.

I got **s**ca**r**ed and had to inqui**r**e a little mo**r**e about that. And I wa**s** g**r**eatly **r**elieved when thi**s** tu**r**ned out not to be the ca**s**e, I wa**s** not in dange**r**, neithe**r** my compute**r**, no**r** my data.

I had to tu**r**n ove**r** again and **r**ead ca**r**efully. Ponoma**r**ev didn't found an attack, actually. What he di**s**cove**r**ed wa**s** a vulne**r**ability, difficult to unde**rs**tand, even mo**r**e to explain. In **s**ho**r**t: mic**r**op**r**oce**ss**o**r** ha**s** a mechani**s**m called **s**ide-channel that, b**r**iefly, expo**s**e any data that an attacke**r** would eve**r** want. It'**s** **r**elated of how mic**r**op**r**oce**ss**o**rs** acce**ss** thei**r** own cache.

**S**o, Ponoma**r**ev wa**s**n't a bluffe**r**, afte**r** all. Actually, he i**s** a b**r**illiant **s**cienti**s**t and **r**e**s**ea**r**che**r**.

And what about hi**s** o**r**iginal p**r**opo**s**al, the one on which thi**s** p**r**e**s**entation i**s** ba**s**ed on?

A**s** I **s**aid, Intel implemented hi**s** idea, but not exactly a**s** he p**r**opo**s**ed at a fi**rs**t moment. The**r**e a**r**e **s**ome diffe**r**ence**s**. They embedded thi**s** mechani**s**m into the GPU, not in**s**ide the CPU. Intel found a **s**olution **r**ega**r**ding pe**r**fo**r**mance, a p**r**oblem that, at **s**ome moment, Ponoma**r**ev **s**tated hi**s** conce**r**n about.

It get**s** mo**r**e technical, but I can only **s**ay that now Intel collabo**r**ate**s** with Mic**r**o**s**oft again**s**t c**r**ypto jacking: Mic**r**o**s**oft Defende**r** fo**r** Endpoint integ**r**ate**s** Intel’**s** **s**ilicon-ba**s**ed th**r**eat detection to advance endpoint detection and **r**e**s**pon**s**e again**s**t c**r**ypto jacking malwa**r**e.

What keep**s** me thinking i**s** if, afte**r** all, deep down, maybe Ponoma**r**ev took hi**s** o**r**iginal idea f**r**om a movie becau**s**e, let'**s** be **r**eali**s**tic: Who don't enjoy a weekend doing nothing but watching movie**s** and enjoying **s**ome popco**r**n?

But it'**s** ju**s**t an idea, i**s** what my imagination offe**rs**. What am I, afte**r** all?

Maybe it'**s** time to thank Hollywood. Who know**s**?

1. Cont**r**a**rr**e**s**ta**r** la**s** amenaza**s**. [↑](#footnote-ref-1)