## CTI-TC Ad Hoc Malware Call

**Meeting Date:** June 2, 2017  
**Time:** 10:00 am EDT  
**Purpose:** Weekly CTI TC STIX SC – Malware Mini Group

### Attendees:

<table>
<thead>
<tr>
<th>Trey Darley</th>
<th>Masato</th>
<th>Richard Struse</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bret Jordan</td>
<td>Ivan Kirillov – Moderator</td>
<td>Sarah Kelly</td>
</tr>
<tr>
<td>Mark Davidson</td>
<td>Gus Creedon</td>
<td>Henry Peltokangas</td>
</tr>
<tr>
<td>Jason Keirstead</td>
<td>Sean Sobieraij</td>
<td>Jane Ginn - Recorder</td>
</tr>
</tbody>
</table>

### Agenda:

- Comments on STIX 2.0 Public Comment period  
- Malware discussion

### Meeting Notes

**Ivan**  
Jason’s concern about embedding Relationship’s in Infrastructure, sync problem  
With Indicator – Not such a problem with Malware

**Bret**  
I don’t know how you build Indicators from some of the things you capture

**Ivan**  
When you start talking about some of the more esoteric stuff, that is true

**Bret**  
From a product POV, we have a few products that sit on the network… but, I don’t see it  
None of the tools I see on network or the endpoint have the ability to look for these things  
Digital forensics is so far ahead of the network tools  
We send a lot of data to SEIM devices, because people want that  
We can’t write a rule for it…can’t do it

**Trey**  
When I was at Splunk and looking at CybOX… my recommendation was do things in 2.1  
And do integrations and close visibility gap by 60%  
-Smart product management  
What is detectible in market today – there are things that should be detectable  
Tomorrow

**Bret**  
Oh, I agree… but when I look at it from an event horizon timeframe… I see that as long term

**Ivan**  
There is the data model and then there is the Patterning – it will take some time to catch up

**Bret**  
I’d like to see Patterning in the market at 60 to 70% Use Case

**Jason**  
What are the things that it is NOT able to do? Has that been enumerated?

**Ivan**  
No, but that is a good idea

**Jason**  
If that is something that can’t be solved… we might need to look at that

**Richard**  
We need to distinguish between those things that are actively looked for by analyst – and MTRI

**Jason**  
We are being pushed more toward analysis and automation

**Bret**  
That is really up to the market – If vendors create products and no-one buys them

**Ivan**  
Balancing act between automation and what we do today
If we can document – then the availability of the data will lead vendors to look at that

This is its own discussion – Future working call –

But, let's go through the comments on the document – Comments from F2F

***If Have Victim Object***

Some fields not necessary – My feeling is that we keep as is

Targeting Oss

Can put in as a Stub

We are causing problems for ourselves with Stubs

That ship has sailed

If we keep these fields – then we can deprecate

We have to be careful about letting the perfect be the enemy of the good
Victim could be industries, technologies, machines, complicated in the short run
If we try to anticipate

Bret – you made a recommendation that we have some guidance on how to handle

More complex items

My question – Why Open Vocab?

We should use the CPE dictionary

Is anyone keeping it up to date?

Is kept up to date – but not complete

Last updated today

Should we do an External Ref?

I did as the software object

One of the downsides does not allow you to reference patch level

You can use wildcards… so you can use it

[More discussion on CPE patterning]

Hard to reference something that is not supported

Everybody uses this… any vendor that has any tool that has to do with vulnerability

Sarah, Do you guys track things on CPE?

I would have to ask our guys at the SOC

I don’t want to get too wrapped up on this – maybe I need to add some examples

I'd say with patches

Next comment I took a stab at enumerating ***architecture***

Should there be an entry for cross-platform?

If I have malware that is Python… then it targets everything
We should make it clear – Targets All? Or analyst does not know what architecture is targeted
We should tell people how to do that

Jason
We could add a field ‘unknown’

Ivan
MISP does that…

Trey
You know what an interesting exercise – to write a program for the MISP guys to look at

Ivan
Do you think they would?

Jason
Pointed out the difference Malware is targeting vs. Malware that is written in a language

Ivan
I’m thinking more about execution

Trey
To Jason’s point – JVM

Jason
What about Malware’s effect on the BIOS – How do we express that?

Ivan
That is a good question. I think of it as a Vulnerability

Rich
Is this more like what we were talking about earlier – with Victim Targeting
We need to clarify that in text

Sarah
Gave example of how a field written in Python – Some analyst’s won’t know that it affects cross

Trey
Maybe we should have some text that makes that explicit

Ivan
We need some examples

Jason
Could it be called ‘Execution Architecture’?

Ivan
Good idea… similarly for Oss
Ok next comment – Trey’s comment – on Artifact Object ***Binary Samples***

Trey
Gave examples of how to handle encrypted files

Bret
Also, the problem where some tools can read zip files – and if it has malware is deleted

Ivan
Are people going to use this for that purpose

Bret
Well, the purpose for STIX

Ivan
So the fact that we have the Artifact Object gets to that point

Jason
I have a question on how to represent the “type Artifact” – References

Trey
Gave example of how to represent it – What do you think of that approach

Bret
Talked about just having an Artifact – We are making you contain an entire Observe_data

Ivan
The reason we did that is because of the graph architecture – Let’s think about Trey’s proposal

Trey
Things always get touchy at the borderline of STIX and cyber_observables

Ivan
If enough commonality, it might work

***String_Patterns***
This could get really messy

Trey

Here I could see something where you have a bunch of indicators that point back

Bret

The reason for Embedded References is so someone cannot add later
Maybe we need to add Yara support

Trey

Mindful of time. We’ll set this as a recurring call at 11:00 EDT

Rich

We’ll also work with Infrastructure during these recurring calls

Meeting Terminated

**************************************************************************************************