FOR IT SECURITY PROFESSIONALS Hyatt investigates malware found on payment processors

Trend Micro: Lessons learned from 2015 cyber attacks

Israeli missile defense chief dismissed for breach of security protocol

December 2015 Issue

Editorial

Let's just call it "The era of IT security"

Subscribe

Archive 

Dr. Peter Stephenson

December 28, 2015

STIX and Taxi - Part 2

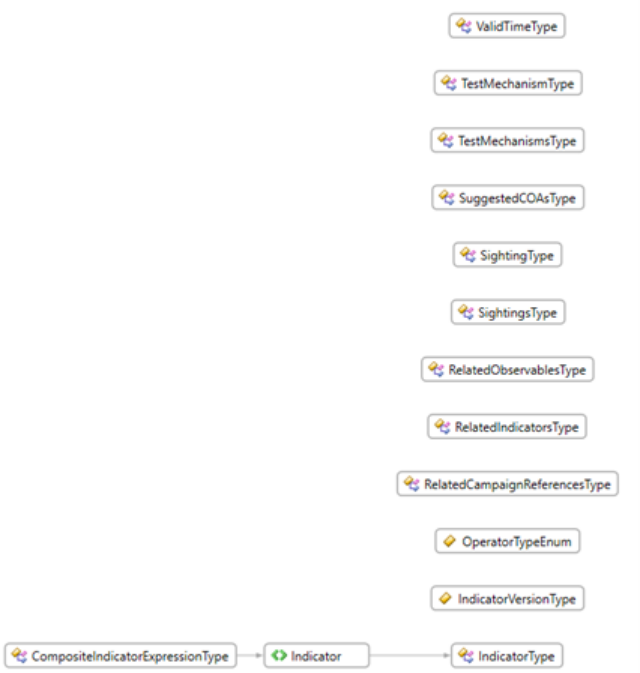
Share this article:

We ended up last time with an introduction to the use of STIX and TAXI for threat hunting. Our last topic was STIX indicators so that's a good place to start this time. I also said that we would look at a campaign, but before we do that we need a little more tutelage on STIX.

As I pointed out, STIX is a flavor of XML. I also mentioned that XML has no pre-defined format so we create schemas to give it the format that we want. We also can make declarations in the schema, but if we want pure STIX files it's better not to. That way when you share with colleagues or try to give it to a device such as a firewall to ingest, you know everything will work. In general, the STIX master schema looks like Figure 1.

Figure 1 - Master STIX Schema Elements

Dr. Peter Stephenson



This is not the XML, obviously. That would take up more space than the blog. However, you easily can see the various elements that make up the master schema. Another way to think about this is that these are the questions you need to answer as you build a STIX characterization. This is just an indicator, remember. Observables, campaigns, actors, etc. each have their own schemas. Let's look at another indicator. This one is a phishing email. Figure 2 shows the tree view of the phishing process and offers some remediation.

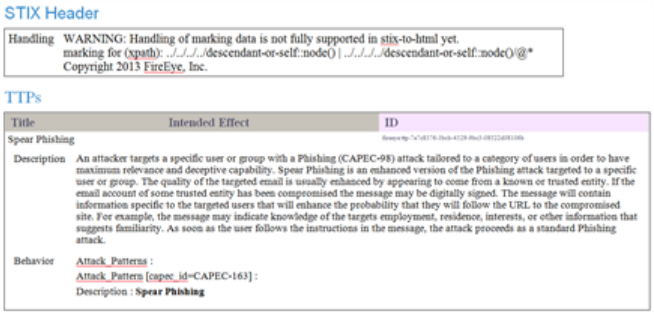
Figure 2 - Phishing Email - STIX Tree View

Notice that we start with the malicious email indicator and that leads to a phishing indicator. That spawns several courses of action (the green boxes), a TTP (tools, techniques and processes) box and an example observable pattern. The TTP also spawns an attack pattern that might be useful as well. Our next stop, logically, is a specific kind of phishing: spear phishing. Since that would not likely stand alone – it probably would be added to the phishing indicator – it's pretty small. The tree view is in Figure 3.

Figure 3 - Spear Phishing - Tree View

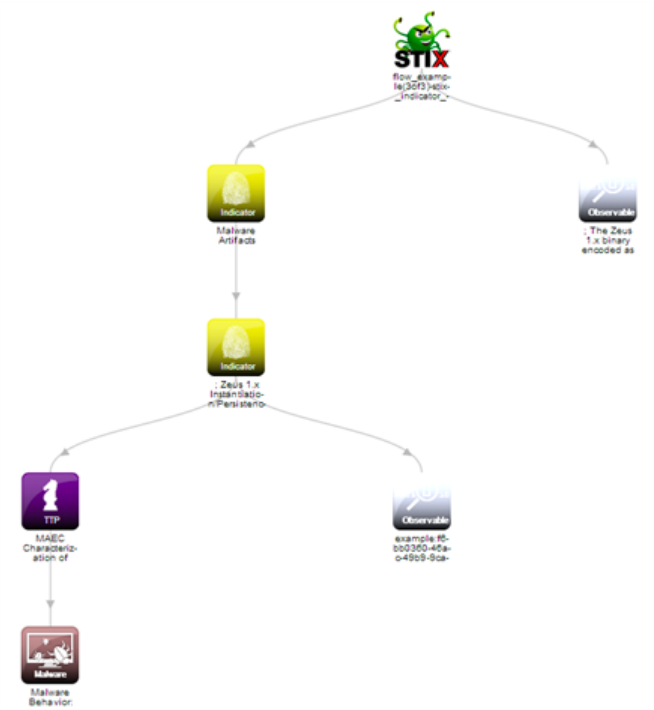
I keep mentioning the XML and we haven't looked at any. XML files tend to be pretty large in the STIX world so we're going to look at some "pretty XML". This has been configured for us by our StixViz viewer. It's in Figure 4 and this is the same STIX file as we saw in the tree view. This STIX file and the subsequent pretty XML is, as you can see, courtesy of our friends at FireEye.

Figure 4 - STIX Spear Phishing - Pretty XML View



It is not uncommon for a spear phishing campaign to lead to the use of malware, so let's look at the tree view of the Zeus banking Trojan in Figure 5.

Figure 5 - STIX Tree View of the Zeus Banking Trojan

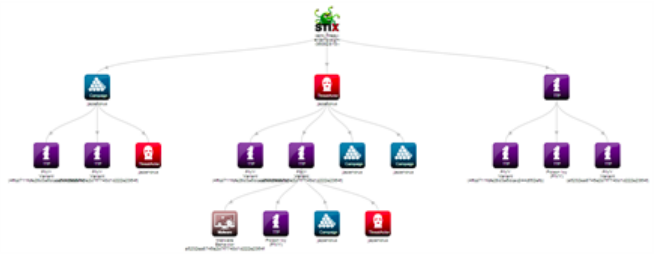


Let's revisit the pretty XML view in Figure 4 for a moment. You will note a new acronym: CAPEC. That is Mitre's Common Attack Pattern Enumeration and Classification. This is a standardized way to describe attacks. The web page at http://capec.mitre.org/data/definitions/163.html gives us the attack pattern for spear phishing. This can be used in characterizing a particular kind of attack in your STIX descriptions.

While we're looking at resources, Mitre has one like CAPEC for us, only this time it is characterizing malware. It is located at https://maec.mitre.org/. MAEC is Malware Attribute and Characterization. MAEC is a language and you'll need to spend some time out on the web site to get familiar with it.

Let's move on, now, to a campaign. We'll just stick our toe in the water this time. Campaigns can get pretty complicated, especially if they go on for a long time and cover a lot of territory. However, they don't have to be. Here's a nice little campaign from an actor named japanorus. You will note, in Figure 6 that this actor is very fond of poison ivy, an old RAT that just won't go away. The main reason is that bad actors can modify it easily in their attempts to bypass discovery and to come up with clever ways to deploy back doors on their victim systems.

Figure 6 - Japanorus Malware Campaign



I've simplified this campaign a bit since it was quite extensive. However, each attack was pretty much the same as all the rest so I just pruned the tree a bit. If we look first at the actor japanorus at the top of the tree, we see that he (I am assuming it's a "he" but it could just as easily be a "she") uses a couple of TTPs and has at least two discrete campaigns showing. If we exploded these we would see that the pattern repeats over and over. He is using poison ivy and at least two variants as we can see from his TTPs. If we looked at the XML – we won't because it's just too big for here – we would see the details of how the campaign was attributed to japanorus, what campaigns actually were conducted and what variants – with hashes – of poison ivy he used.

That's a lot to swallow this time. Next time we will begin the first of two dives into a really big campaign – the APT1 Campaign courtesy of Mandiant and FireEye. This one is huge and we'll just look at some of the characteristics of a campaign carried out using APTs.

Before I go, though, here is a new feature that I will try to do for you weekly. This one is courtesy of Malware Domain List - http://www.malwaredomainlist.com/ - and it will include the malicious domains added to the Malware Domains List in the past week. That should provide some opportunity for you to block – or, at least, recognize - some bad actors. For more information – a lot more, really – go out to the web site. Here's this week's list:

Domain	IP	Reverse Lookup	Malicious Content
www.schluckspecht.com/	62.75.229.120	titan464.startdedicated.net.	compromised site leads to Angler EK
www.agrimont.cz/	95.168.204.225	masakrator.zikum.cz.	compromised site leads to Angler EK
www.ax-electronic.de/	81.169.145.172	wac.rzone.de.	compromised site leads to Angler EK
www.wohnmoebel-blog.de/	85.13.147.213	dd29530.kasserver.com.	compromised site leads to Angler EK
www.mangiamando.com/	81.31.147.60	jmhlmd14.colt-engine.it.	compromised site leads to Angler EK
www.schillinger-beregnungsanlagen.de/	213.214.28.47	28-47.rzfr.de.	compromised site leads to Angler EK
pepol.flaviocastro.eu/	162.216.6.171	newserver.datadns100.com.	Paypal phishing
www.lambrusco.it/	95.110.174.125	kscrb.kosmosol.it.	compromised site leads to Angler EK
www.bergsaker.se/	62.119.81.150	flava.se.	compromised site leads to Angler EK
www.tzwl.de/	85.214.103.1	tzwl.de.	compromised site leads to Angler EK
www.diamondgrp.co.uk/language/en-GB/ppl/usam7/	75.125.234.114	mx1.vitay.info.	Paypal phishing
www.diamondgrp.co.uk/includes/phpmailer/index.htm	75.125.234.114	mx1.vitay.info.	Paypal phishing
eeps.me/	208.67.23.26	h155.cpanellogin.net.	ESET phishing
imagesrv.onestate9786.com/info.php	74.117.183.100	100.64/26.183.117.74.in-addr.arpa.	Teslacrypt ransomware c&c

So… until next time….

--Dr.S

If you use Flipboard, you can find my pages at http://tinyurl.com/FlipThreats. Here I flip the interesting threat-related stories of the day – nothing particularly technical, but interesting stories none-the-less.

Hunting and STIX