[9] *Modelling Disruptive APTs targetting Critical Infrastructure using Military Theory*

Yoram Meijaard (TNO and TU Eindhoven), Peter-Paul Meiler (TNO) and Luca Allodi (TU Eindhoven).

Reviews Phase 1

Review 1

Time: Jun 04, 08:57

Overall evaluation: 0 (borderline paper)

This paper presents a review of the evolution of the existing APT kill chain model, together with a model of so-called Disruptive APTs (D-APTs) that target critical infrastructures. The proposed model describes a number of features design to model D-APTs that range from the setting of strategic objectives to those aiming at characterizing the societal function.

Strengths: - Relevant Problem - Good Review

Weaknesses: - Novelty - Lack of evaluation - Scope within APT

Comments:

The paper is well written and easy to follow. The authors have done a good review of existing works in the area. The contribution is clear and I particularly appreciated the effort put by the authors in mapping the phases of D-APT into existing TTPs, which is summarized in Table III. Judging by this table, it is clear that the D-APT kill chain is either more generic (gathers attributions from different categories like Discover, Collection, etc) or it breaks down categories into specific ones (e.g., lateral movement and pivot).

Disruptive attacks by nature have an effective duration of months as opposed to persistent threats. It would have been good to offer a discussion on whether disruptive attacks should at all be considered a type of APT due to their limited persistence. I feel there is a tension between the level of descriptiveness and the long-term nature of APTs.

Authors argue that related work does not capture elements of CI (Critical Infrastructures) in their models, except for the ICKC (Industrial Control Systems Cyber Kill Chain). One of the main limitations of ICKC is that it does not describe how an attacker got to the ICS system. However, traditional models like the Cyber Kill Chain are designed to precisely explain this. Instead, the authors model the CI after existing work: [4] (societal), [27] (process), and [28] (technical). The quality of the paper would improve if authors were to position better their contribution w.r.t. the SOTA.

Perhaps one of the main weaknesses of this paper is that it does not show how effective this model is in modeling CI threats. Having a number of case studies showing the benefits of the proposed model w.r.t. existing ones would considerably improve the quality of the paper.

Looking at the disruptive APT model, I was left to wonder about the rationale of the different levels. For instance, it is unclear why it is important to model the rehearsal operational level. Here, readers may wonder how characteristics that fit into the rehearsal level can be used to produce actionable threat intelligence. It is also unclear why Figure 6 depicts levels in blocks of four levels that are intertwined? Why weaponization and rehearsal are in the same (yellow) category? It looks like the same set of colors is used in Figure 7 when representing TTPs, is this connected?

Reviewer's confidence: 3 (medium)

Review 2

Time: Jun 08, 20:43

Overall evaluation: 1 (weak accept)

This paper presents a new kill chain model for disruptive APTs (DAPTs). The authors argue that previous models only took into account APTs focused towards exfiltrating data. However recently we are seeing more and more APTs targeting the critical infrastructure with a goal of sabotaging this or disrupting this, therefore new models are needed.

The authors perform a literature review of research on both APTs and critical infrastructure. When performing a systematic review it is customary to explain how the papers were identified. Did the authors perform queries or search engines or did they start from a set of recognized publications venues and expanded? This would help the reader understand how comprehensive the literature review is.

The proposed model is interesting, I like the application of military theory to APTs and the split between different levels (strategic, operational, tactical). I think that this model adds on traditional kill chain based models, and it could inform additional research in this space as well as spark interesting discussions at the workshop.

The authors correctly acknowledge the limitation of their approach, which is that this model is not validated by data. This could however be the focus of future work.

Reviewer's confidence: 3 (medium)

Rebuttal Letter

We would like to thank the reviewers for their time, suggestions and comments. We will summarise the comments and provide a point-to-point response.

The main critique from both Reviewer 1 and Reviewer 2 indicates the lack of use cases showing the benefit of the proposed model. The goal of this paper is to provide a cross-disciplinary evaluation of the (D-)APT literature to derive a general model for future evaluation. As such, we agree with R2 that an extensive evaluation with multiple use-cases can be left for future work; on the other hand, since the reviewers feel strongly about an at least illustrative application of the model being reported in the paper, we are confident we can include one on the D-APT BlackEnergy3 in the revised version. We should mention that including such a use-case, even at this illustrative level, will be a substantial addition to the paper (about half a page) and might require additional attention later in the review process.

The remaining, relatively minor, comments from the reviewers are straightforward to address in the paper:

Reviewer 1 suggests to discuss whether disruptive attacks should be considered a type of APT, and to clarify the paper’s position in the SOTA, in particular with respect to ICKC.

Regarding the first point, there is indeed a difference in mode of operations, yet the attackers share similarities too e.g. the attacks are highly sophisticated and executed by similar – if not the same – actors. We will expand on this similarity and further clarify the differences.

On the second point, the reviewer is correct in their view of the ICKC. However, this does not conflict with the claim that only the ICKC specifically considers CIs (but does not tell how to reach them). We will clarify the distinction. Moreover, this indicates an area of improvement in our comparison to the SOTA.

Reviewer 2 also suggests to include the searching methodology and details. We kept track of the search queries and methodology, and we can include details on those in the paper revision.

Remaining comments on clarifications for the levels (e.g., strategic, operational and tactical) and colour scheme are also helpful in improving the paper, thank you.

We thank again both reviewers for their very insightful comments.

Reviews Phase 2

Review 3

Time: Jun 27, 12:03

Overall evaluation: -2 (reject)

The paper addresses an interesting topic, but it fails to properly motivate what specific problem of existing attack models it tries to solve. As such, it contributions are unclear to me.

Overall, I'm not entirely sold out by the message that D-APTs are a special type of attack that deserves their own model. Disruption is just one possible impact that fits perfectly existing models. Even in the case of CIs, disruption could be achieved with almost no sophistication, as demonstrated by the recent incident on the Colonial pipeline that caused panic buying among some populations since filling stations were without fuel for several days.

The paper's main motivation ("no existing APT model incorporates the disruptive actions of D-APTs", 2nd par in the introduction) is not true. One of the standard methodologies to model kill chains, MITRE's ATT&CK matrix, incorporates one technique that models the impact of the attack and explicitly covers many forms of disruption (see https://attack.mitre.org/tactics/TA0040/). In the specific case of Industrial Control System, the corresponding ATT&CK matrix characterizes and describes various forms of disruption within the impact techniques (see https://collaborate.mitre.org/attackics/index.php/Main_Page). What surprises me is that the authors mention ATTA&CK in Section V and even map

By the end of the paper, the authors argue that there is a lack of empirical data to validate the results. But they mention three well-knwon examples: Stuxnet, BlackEnergy3 and Industroyer. I suggest you take the opposite road to motivate the paper: model those APT instances in existing attack modeling frameworks and use the results to motivate why do we need a new model that overcomes the deficiencies that you have found.

Reviewer's confidence: 3 (medium)

Review 4

Time: Jun 29, 13:21

Overall evaluation: 0 (borderline paper)

This paper presents a conceptual analysis of a new form of attack, the Disruptive Advanced Persistent Threat, which presents a different threat to critical infrastructure than earlier APTs. The D-APT also have a different modus operandi than other attackers.

The paper feels like it is aiming to be comprehensive, while for this workshop there is a limited length. I feel the actual contribution of the paper suffers because of it. It also feels like the authors felt themselves forced to overuse abbreviations, which makes this paper very hard to read. I am aware that the subject field of this research often uses abbreviations for regularly used concepts (APT, ATT&CK, OODA, ICS, etc.), but then the authors introduce even more abbreviations for concepts that are not regularly abbreviated (CI, CP, CKC, etc), and it also does not help that they regularly refer to TTP instead of using a more general term.

The contribution in Section IV Modelling CI seems to be very limited. The introduced model is not a particularly groundbreaking new insight, nor does it seem particularly important to the rest of the paper. I can see the value in using it to describe D-APTs, but I would not call this a new "CI model".

The paper uses a lot of space to describe why the D-APT should be modelled in this way, and it presents a clear case that this is a new phenomenon. But the discussion on the actual contribution of this model is only very minor, and I feel that that there is much more to be gained from having the thoughts from the authors in that regard.

Reviewer's confidence: 5 (expert)

Review 5

Time: Jul 02, 10:48

Overall evaluation: 0 (borderline paper)

=== meta review ===

The PC agreed that the paper has potential for publication, but the following issues must be addressed before it is ready for publication:

1. Provide a case study to motivate and justify the need for a D-APT model. Include an explicit comparison with the ATT&CK model (R1, R3) 2. Improve the readability and try to tone down the amount of abbreviations (R4)

Reviewer's confidence: 5 (expert)