Attacking Operational Technology Without Specialized Knowledge The Unspecialized OT Threat Actor Profile

DECISION: Accept

AUTHORS: Stash Kempinski, Savio Sciancalepore, Emmanuele Zambon and Luca Allodi

Summary of Reviews

- Review 1: 0 (3)
- Review 2: 2 (4)
- Review 2: 3 (4)

Reviews

Review 1

Total score: 0

Overall evaluation: 0

Reviewer's confidence: 3

This paper characterizes the profile on an unskilled ICS attacker. The paper argues this persona has accounted for a significant portion of reported ICS attacks since 2010.

* There's a difference between "had limited capabilities" which is the persona illustrated through individual anecdotes, and "used limited capabilities" which is the categorization defined through tool identification. There are plenty of reasons why more capable attackers would prefer simple tactics.

* The choice to not include motivation in the persona makes it harder to reason about specific instances of what an unskilled attacker might look like. Perhaps a breakdown of associated motivations could be useful in further refining the attacker model.

* In 6.1 you say "Our keywords had a low hit rate, as further discussed in Section 6.3". Section 6.3 does not provide additional detail on the keywords searched specifically, but rather on the tools discovered. More methodology on the choice of keywords searched, and how threads were filtered would be helpful in gaining confidence in the assertion that tools were not present, as opposed to not discovered, on the forums.

* The naming of markets only in appendix D is probably not needed / can be edited.

Review 2

Total score: 2

Overall evaluation: 2

Reviewer's confidence: 4

#7: Attacking Operational Technology Without Specialized Knowledge: The Unspecialized OT Threat Actor Profile

The paper provides an interesting and useful characterisation of the Unspecialised OT Threat Actor (UOA) Profile with a categorisation of publicly known attacks to substantiate whether the UOA threat is a real problem and to provide some evidence that it is an increasing problem.

In 3.1 I don't really understand the reasoning behind avoiding a 'dual-use' classification. Many tools are dual-use e.g. nmap/metasploit. Those tools themselves are not malicious though they are often used maliciously while e.g. Zeus is malicious in nature as it doesn't have benign use cases. This definition is important as if a security practitioner is found to have some "malicious" tools in their possession then they would have some serious justification to do to avoid a criminal prosecution, but if they are dual-use then stating that they used them as part of their work as a security practitioner would be fine (under my understanding of UK law).

End of 3.1 "only be obtained" that is quite a strong statement, usually second hand markets exist outwith the control of the vendor and so while it is difficult to obtain such equipment without going through the vendor it is not impossible, and vendors don't necessarily do strong checking on customers beyond their ability to pay.

6.1 It is unclear to me how naming the forums would identify the authors as they are presumably widely used forums that many others could have accessed. There are also many datasets of cybercrime forums available, e.g. through the Cambridge Cybercrime Centre and so expanding the search across more forums is not difficult (if time consuming to process the additional results). There might be other good reasons for not naming them though. This was not clarified by Appendix D.

It might be helpful to quantify how many results you got and how many seemed relevant based on the titles. Probably that information is no longer available though.

6.2 Here also a PRISMA style breakdown of how many entries there were before each stage of filtering would be helpful.

A good set of recommendations though the practical implications could be made more explicit.

Good effort towards reproducibility with the data being made available.

Minor comments

Bottom of page 1 "OT(-components)," ? Also not sure "amount" is the right word later in that paragraph, "proportion" or "number"? "Amount" feels more continuous and tools are discrete.

Potentially relevant (but not necessary). The security economics arguments it contains might strengthen your argument: "When will my PLC support Mirai? The security economics of large-scale attacks against Internet-connected ICS devices" Dodson et al. https://ieeexplore.ieee.org/document/9493257

p5 footnote 2 the formatting is off, the 2 should come after the punctuation and there should be a space first. Footnote should begin with a capital letter.

Figures 1 and 2. The font size is too small for some aspects and should match that of surrounding text.

For Figure 2 it might be better to put the legend on the bottom as you don't have much width to play 1twith in a 2 column format.

The CRUD acronym is only expanded in Appendix C. In general it might be helpful to do a thorough check for acronym use to ensure they are expanded, perhaps use a LaTeX acronym package to ensure you always get it right.

Review 3

Total score: 3

Overall evaluation: 3

Reviewer's confidence: 4

This paper breaks current assumptions about the capabilities and strategies of cyber attackers being highly sophisticated and using exquisite tools. Instead, this papers presents -- and tests -- a hypothesis that instead of fitting this pattern, cyber attackers targeting OT systems employ only basic skills and capabilities.

It is important to separate two ideas: unspecialized actors who use sophisticated tools (that someone else has developed), and unspecialized actors who use unsophisticated tools.

Overall, it is a really interesting paper that contributes to a massively understudied area of theories (and evidence) about attacker behavior.

The data present limitations for generalization of the insights (external validity), but nevertheless, this is a nicely structured approach and paper.

Given very recent work by researchers using LLMs to craft exploits, I wonder how that will change further cyber attacks, especially those on OT. Moreover, I wonder if exploits generated by LLMs could be detected and identified as being developed by LLMs.