Killed In Translation

silascutler.com/2021/01/14/KilledInTranslation/

January 15, 2021

2021-01-14

Preface:

A director at Google once told me that the larger an organization, the less subtlety is possible in what it says publicly, and even the most carefully postulated assessment, cushioned with supporting analytic language, will be interpreted as fact.

Naming of threat actor groups and malware is a critical aspect to tracking cyber operations. Armchair Researchers, more concerned with social media follower counts, often decry these names as marketing hooks, whereas they are actually complex shibboleths that convey the scope of a set of activity and its sourcing.

Since roughly 2016, the United States government has been actively working to collaborate with non-government agencies. The National Security Agency (NSA), Cybersecurity and Infrastructure Security Agency (CISA), and the Federal Bureau of Investigation (FBI) have all begun publicly sharing tactical reporting containing technical details, indicators, and defensive recommendations. These reports have become a staple of any major cyber incident because they provide an authoritative situational overview and an initial starting point for collaboration.

In recent reports[1][2], attribution has been presented at the forefront of the report and used industry cryptonyms along with military units or specific government entities. While this may be intended to support broader usage (outside of technical consumers), attribution in these reports, without supporting analysis, is creating a dangerous precedent.

Technical analysis is fundamentally rooted in scientific methodology. When research is presented, a basic requirement is that it is sufficiently detailed to be validated by reproducing the analysis. Within the aforenoted reports, attribution is presented as a statement of fact, similar in confidence to the reported dates or software versions, instead of as a confidence-structured assessment.

It may be possible the authors of these reports have a Palantír[3], allowing them to perfectly identify the hostile authors, but without proper confidence language and presentation, these assessments are just as likely to have been made by a roll of the dice.

In future reports, providing context regarding how reported activity links to named sets will provide critical information to existing understanding of these groups. In instances where providing this information may risk sources and methods, limiting assessed attribution to a broad geographic estimate or omitting it entirely may provide a better service.

[1] https://media.defense.gov/2020/May/28/2002306626/-1/-1/0/CSA%20Sandworm%20Actors%20Exploiting%20Vulnerability%20in%20Exim%20Transfer%20Agent%2020200528.pdf
[2] https://media.defense.gov/2020/Jul/16/2002457639/-1/-1/0/NCSC_APT29_ADVISORY-QUAD-OFFICIAL-20200709-1810.PDF
[3] https://en.wikipedia.org/wiki/Palant%C3%ADr

Older
Backdooring a HID Reader