Recommended Revisions To The Wassenaar Arrangement

03/18/16

Thank you for considering Rapid7's 2015 comments to the Dept. of Commerce's Bureau of Industry and Security (BIS) proposed rule to implement the Wassenaar Arrangement.[1] Because a US implementation rule would not apply to other parties to the Wassenaar Arrangement, and because cybersecurity is a global enterprise that routinely requires cross-border collaboration, Rapid7 urges BIS and the Dept. of State to renegotiate the core text of the Wassenaar Arrangement itself rather than addressing the challenges solely through a US implementation rule. Revisions to the Wassenaar Arrangement should be made with broad consensus among industry, researcher, and other cybersecurity stakeholders.

Rapid7 supports stripping provisions 4.A.5, 4.D.4, 4.E.1.a, and 4.E.1.c from the Wassenaar Arrangement as the preferred solution.[2] If stripping the provisions is not possible, we suggest considering the below modifications – deletions in strikethrough and additions in red – to the Wassenaar Arrangement's core language.[3]

i) Exceptions to the controls on software, systems, and technology[4]

4.D.4. "Software" specially designed or modified for the generation, operation or delivery of, or communication with, "intrusion software".

Note: 4.D.4 does not apply to "software" specially designed to be installed or used with authorization by administrators, owners, or users for the purposes of asset protection, asset tracking, asset recovery, or 'ICT security testing'. "Software" shall be deemed "specially designed" where it incorporates one or more features designed to confirm that the product is used for security enhancement purposes. Examples of such features include, but are not limited to:

a. *A disabling mechanism that permits an administrator or software creator to prevent an account from receiving updates; or*

b. *The use of extensive logging within the product to ensure that significant actions taken by the user can*

---

[1] Rapid7, Comments to BIS Proposed Cyber Rule, Jul. 24, 2015, https://community.rapid7.com/servlet/JiveServlet/download/7173-1-27375/Rapid7%20-%20Comments%20to%20BIS%20Proposed%20Cyber%20Rule_final.pdf.

[2] The Wassenaar Arrangement on Export Controls for Conventional Arms And Duel-Use Goods And Technologies, List Of Dual-Use Goods And Technologies (WA-LIST), Mar. 12, 2015, pgs. 72-73, http://www.wassenaar.org/wp-content/uploads/2015/08/WA-LIST-15-1-2015-List-of-DU-Goods-and-Technologies-and-Munitions-List.pdf#page=72

[3] This suggested language is drawn in part and modified from Thomas Dullien, Vincenzo Iozzo, and Mara Tam, *Surveillance, Software, Security, and Export Controls* (Draft Report), Feb. 10, 2015, pgs. 8-9, https://tac.bis.doc.gov/index.php/component/docman/doc_view/299-surveillance-software-security-and-export-controls-mara-tam#page=8.

[4] See WA-LIST, pgs. 72-73. The goal is to exclude legitimate cybersecurity products from the control while still encompassing items particularly prone to malicious use. Note that this proposed language is not based solely on the intent of the exporter that the software or system be used for security enhancement – instead, this proposed language would apply to software or systems *designed* to carry out that intent, which is a more objective and technical measure than intent alone. We include examples (in 4.D.4a-b) of software design features that might qualify, which could be included in either the Arrangement text itself or an implementing rule.

be audited and verified at a later date, and a means to protect the integrity of the logs.

4.A.5 Systems, equipment, and components therefor, specially designed or modified for the generation, operation or delivery of, or communication with, "intrusion software".

Note: 4.A.5 does not apply to systems, equipment, or components specially designed to be installed or used with authorization by administrators, owners, or users for the purposes of asset protection, asset tracking, asset recovery, or 'ICT security testing'.

~~4.E.1.c. "Technology" for the "development" of "intrusion software".~~

ii) Modify the definition of "intrusion software" to focus on lack of authorization[5]

Cat 4 "Intrusion software"

1. "Software"

a. specially designed or modified to avoid detection by 'monitoring tools', ~~or~~ to defeat 'protective countermeasures', or to be run or installed without the authorization of the user, owner, or 'administrator' of a computer or network-capable device, and

b. performing any of the following:

~~a.~~1. The unauthorized extraction of or denial of access to data or information from a computer or network-capable device~~, or the modification of system or user data~~; or

~~b.~~2. The unauthorized modification of ~~the standard execution path or a program or process in order to allow the execution of externally provided instructions~~ system or user data to facilitate access to data stored on a computer or network-capable device by parties other than parties authorized by the owner, user, or 'administrator' of the computer or network-capable device.

iii) Modify the notes to the definition of "intrusion software" to exclude security testing and software distributed for security purposes[6]

Notes

1. "Intrusion software" does not include any of the following:

a. Hypervisors, debuggers or Software Reverse Engineering (SRE) tools;

[5] See WA-LIST, pg. 210. These modifications help distinguish features of intrusion software that can be used for malicious purposes. However, these modifications alone would be insufficient to protect cybersecurity because software shared for legitimate purposes, such as exploits identified by researchers, could still qualify as "intrusion software" even under this modified definition since many exploits are designed to be installed without authorization.
[6] See WA-LIST, pg. 210.

b. Digital Rights Management (DRM) "software"; ~~or~~

c. "Software" designed to be installed or used with authorization by manufacturers, administrators, owners, or users for the purposes of asset protection, asset tracking ~~or~~, asset recovery~~.~~, or 'ICT security testing'; or

d. "Software" that is distributed, for the purposes of helping detect or prevent its unauthorized execution, 1) To organizations conducting or facilitating research, education, or 'ICT security testing', 2) To Computer Emergency Response Teams, 3) To the creators or owners of products vulnerable to unauthorized execution of the software, or 4) Among and between an entity's domestic and foreign affiliates or subsidiaries.[7]

Technical Notes

1. Monitoring tools': "software" or hardware devices, that monitor system behaviours or processes running on a device. This includes antivirus (AV) products, end point security products, Personal Security Products (PSP), Intrusion Detection Systems (IDS), Intrusion Prevention Systems (IPS) or firewalls.

2. 'Protective countermeasures': techniques designed to ensure the safe execution of code, such as Data Execution Prevention (DEP), Address Space Layout Randomisation (ASLR) or sandboxing.

3. 'Authorization' means the affirmative or implied consent of the owner, user, or administrator of the computer or network-capable device.[8]

4. 'Administrator' means owner-authorized agent or user of a network, computer, or network-capable device

5. 'Information and Communications Technology (ICT) security testing' means discovery and assessment of static or dynamic risk, vulnerability, error, or weakness affecting "software", networks, computers, network-capable devices, and components or dependencies therefor, for the demonstrated purpose of mitigating factors detrimental to safe and secure operation, use, or deployment.[9]

We would be pleased to discuss these and other recommendations further. Thank you for your consideration.

END

[7] These modifications in (d) are important in order to avoid classifying exploits shared for cybersecurity purposes, such as research and education, as intrusion software. For example, a German researcher discovers a vulnerability in a consumer software product, and she shares a proof-of-concept with 2) CERT, and 3) a UK company that owns the flawed product; the UK company then shares the proof-of-concept with 4) its Ireland-based subsidiary, and 1) Rapid7, based in the US, to conduct ICT security testing. Note that this suggested language is also not solely based on the purpose for which the "intrusion software" was shared – the language describes particular end users, which is a more objective criteria than intent alone.

[8] We intentionally did not limit authorization to "informed consent" in order to avoid making the "intrusion software" classification contingent on the end user's degree of understanding, rather than whether the end user has provided consent.

[9] This is a key definition. We recommend confirming with other stakeholders that it adequately captures the range of activities that should be excluded from control under the Wassenaar Arrangement.