FireEye

Unintended Consequences

The Adverse Effect of Wassenaar on Victim Notifications

Written Comments for
BIS RPTAC Meeting
8-December-2016

SECURITY

FireEye

CONTENTS

Introduction

FireEye, a global information security company, constantly works to improve the security posture of their customers and a wide variety of other entities by contributing positively to the global security community. The ability to freely share and transmit information about undocumented software vulnerabilities, exploitable versions of which are sometimes referred to as "zero days," and other malicious software considered "Intrusion Software" is a major part of this effort.

This whitepaper will illustrate a case study drawn from real life events, and then discuss how:

- The free transfer of information concerning undocumented software vulnerabilities is critical to collaborative efforts to improve security
- The example outlined in the study is but one instance of how FireEye regularly conducts business and works with external entities
- How restricting these conversations will damage US commerce while benefitting other organizations that are not bound by similar restrictions.

Executive Summary

As currently written, the proposed language in the Wassenaar agreement would restrict or deny the ability of FireEye to communicate with victims of compromises or exploits that are outside of the United States. This is illustrated by a case study taken from real events in 2015.

Restriction of the ability to freely share and transmit information about exploits, intrusion software, and/or their surrounding ecosystems will hamper the abilities of not only FireEye, but also many other major contributors in the information security industry in the United States. Taken to an extreme, this would have a chilling effect on innovation and commercial growth of US companies, due to this being a core component of how many information security companies do business.

Zero Day Notification, a Case Study

As part of their regular business practices, FireEye routinely notifies victims of malicious actors, activities, and campaigns that are detected by FireEye's technologies, consultants, and intelligence and research organizations. What follows is a summary of one such notification and additional activities that followed.

- In 2015, FireEye researchers identified what they believed was the active exploitation of an undocumented software vulnerability by malicious threat actors.[1]
- FireEye researchers confirmed that this was indeed a repeatable exploit in software sold by a vendor who was not a FireEye customer, and was not based in the United States.
- FireEye then notified the software vendor of the existence of the software vulnerability.
    - **The discussions around the notification consisted of transferring information about the "zero day" exploit and the ecosystem surrounding the use of the exploit to a foreign entity with no pre-existing relationship with FireEye.**
    - Simultaneously, FireEye researchers continued to work on further documentation of the exploit, as well as protection for FireEye customers.
- The non-US software vendor then quickly developed a patch for vulnerability and released it to their customer base to protect against the malicious campaign.
- After the patch was released, FireEye published their research findings to inform other organizations affected, and the security community as a whole.[2] This was done in a responsible & coordinated manner ONLY after the earlier discussion with the vendor had been completed and the vendor approved of this publication.

During the events described above, FireEye was able to quickly determine a new exploit was being used actively by malicious actors, and notify a software vendor outside the United States with whom there was no formal pre-existing relationship. This prompt notification and discussion of the vulnerability then led to a patch being developed, which benefitted all users of that company's products, not just FireEye customers.

---

[1] There was no previous public knowledge of this software vulnerability, and no active patch for this existed, thus this vulnerability would be considered a "zero day" vulnerability.

[2] https://www.fireeye.com/blog/threat-research/2015/09/zero-day_hwp_exploit.html & https://www.fireeye.com/content/dam/fireeye-www/global/en/blog/threat-research/FireEye_HWP_ZeroDay.pdf

The Impact of Wassenaar on Notification

The lifecycle of the events in the previous case study elapsed in a period of eight days, from the discovery of the vulnerability by FireEye to the issuance of the patch by the vendor. Assuming implementation of the currently proposed Wassenaar language, the transfer of information outlined in the case study would NOT have been covered by any pre-existing licensing agreement between FireEye and their customers, nor would any deemed export licensing have covered it. There was no formal pre-existing relationship between FireEye and the software vendor in this case study before the discovery of the vulnerability.

Additionally, granting licensing for information transfer about exploitable undocumented software vulnerabilities ("zero-day exploits") are "presumptively denied" as a class, which implies that a license would likely not be granted in any case. Stopping before notification in the preceding case study workflow would create the following situation:

- FireEye could not notify the vendor in a responsible manner.
- The vendor would not know to develop a patch.
- Customers of the vendor would still be actively exploited, unless they were customers of FireEye.
- Information about the incident would not be published to the security community so that vulnerable parties would not know to patch, and researchers could not learn from this incident.[3]

Assuming that that the "presumptive denial" portion of the language is struck out, FireEye would still have to have applied for a license for this specific conversation, which is time and resource consuming. This introduces the following additional complications:

- The Level of Effort to conduct the notification increases greatly.[4]
- The time to notification is increased while waiting for the license to be granted.
    - With this increase, the window of exploitation potentially goes from days to months, during which malicious actors are unchecked.
- The vendor may not wish to deal with a notification that involves the conversation being registered with the United States Government, and may dismiss the overture out of hand, which is the same as if the notification could not occur (see above).

---

[3] Information in the public domain is an exemption to licensing, but it could only be responsibly published if the earlier conversations had taken place. Without that, publishing this information is not responsible/coordinated disclosure.

[4] Greatly, because the personnel usually conducting notifications are usually Subject Matter Experts, whose time is very valuable and are not easily hired or replaced. These SMEs now have to engage an entire additional tier of staff to seek government licensing, and then spend time making sure it is in order before they can proceed.

FireEye: Notifications as a Way of Life

The act of notification is a core component of how FireEye and other research driven security companies conduct business – it is the fruit of a variety of research, development, and intelligence functions inside of FireEye, taking the ability to find and detect threats before they are publicly known and using that to help others. Notification allows FireEye to assist and improve the security posture of entities that are NOT existing customers (but may be very important in their own industries or markets, and affect many other consumers, corporations, or governments around them), as well as grow business and relationships throughout the world that allow FireEye to continue to succeed as a US-based industry leader.

The unintended consequences outlined in the case study would be bad enough if that were an isolated incident, but FireEye discovers multiple undocumented software vulnerabilities every year, and works to responsibly disclose them as quickly as possible for the betterment of all involved. Additionally, FireEye routinely notifies external entities outside of the US in conversations that may involve either undocumented software vulnerabilities or "intrusion software" and their surrounding ecosystems on a regular basis. **So far in 2015, FireEye has attempted 50 notifications of organizations that are outside of the United States, any or all of which may have contained items that would trigger restriction and/or a requirement for licensing under the current Wassenaar language.**

The notification process is not always to a software vendor (as outlined in the case study above), but may be to another significant entity that our research shows is currently being actively exploited. These include major foreign companies, governments, and non-government. Many of these entities are in countries that regularly trade and do commerce with the United States or US companies or consumers, and their continued exploitation can have an adverse effect on any other organizations that interact with them.

Conclusion

Without the ability to have unfettered conversations during the notifications process, FireEye would lose the ability to effectively communicate with many of these foreign entities, and thus lose opportunities to stop active exploitation of both vulnerabilities and entities by malicious actors. The information being exchanged in these conversations is not for the oppression of private citizens, or to supply malicious actors with the ability to act on the exploits, but rather to document and demonstrate malicious campaigns that are current threats to a variety of different types of victims. Without this ability, FireEye and other companies like it would lose their ability to increase the security posture of Internet citizens on a global scale, and the role would move to companies based in countries that were not bound by such restrictions.