



Staffan Truvé, CTO & Co-founder
Recorded Future

NVD – Too Little, Too Late?

Vulnerability Management

- Tracking vulnerabilities and acting to reduce the threat they pose is a key part of security
- Vulnerability databases such as NVD and CNNVD are key to staying informed
- However, they cannot be the only way – since they are sometimes slow, and sometimes unreliable
- Our study of CNNVD led to some interesting observations...



Nomenclature

- CVE – Common Vulnerabilities and Exposures dictionary
 - Administered by MITRE
- NVD – National Vulnerability Database
 - CVE augmented with additional analysis
 - Administered by NIST
- CVSS - Common Vulnerability Scoring System
 - An open standard for assigning vulnerability impacts
- CNNVD – Chinese Vulnerability Database
 - Chinas corresponding database
 - Administered by?

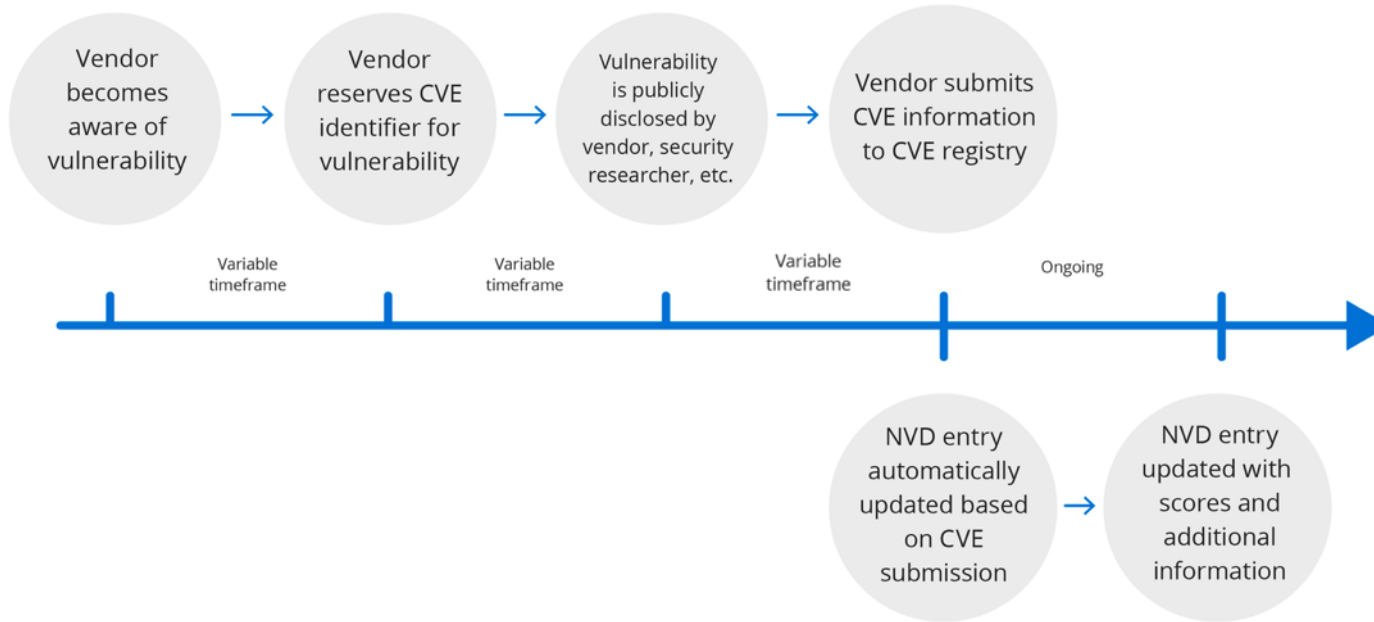


NVD –
Too Little, Too Late?



Recorded
Future

CVE Submission Process

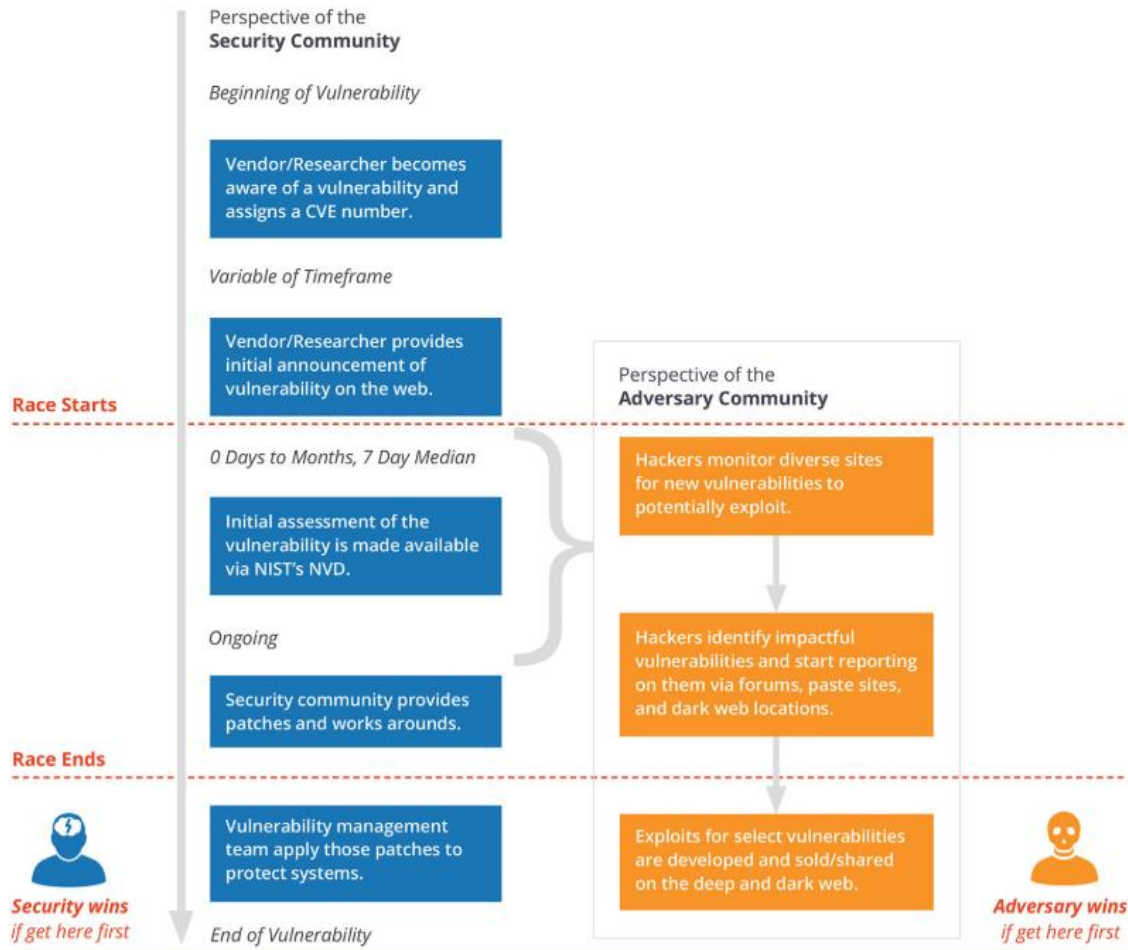


NVD Process

NVD –
Too Little, Too Late?

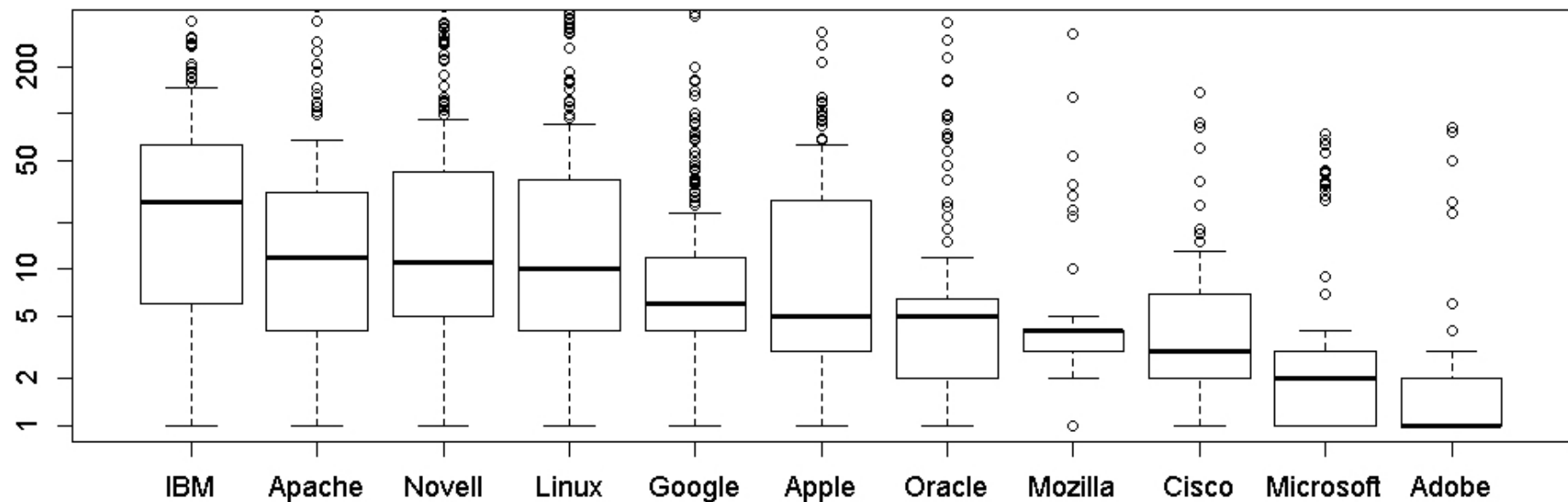


Recorded
Future



NVD –
Too Little, Too Late?





1 Insikt Group Note

100+ References to This Entity

First Reference Collected on May 8, 2018

Latest Reference Collected on May 11, 2018

★ Curated Entity



Critical

Risk Score 89

5 of 18 Risk Rules Triggered



Spike in cyber references in the last 60 Days

[Information Technology Laboratory](#)

NATIONAL VULNERABILITY DATABASE

VULNERABILITIES

CVE-2018-8174 Detail

AWAITING ANALYSIS

This vulnerability is currently awaiting analysis.

Description


A remote code execution vulnerability exists in the way that the VBScript engine handles object Remote Code Execution Vulnerability." This affects Windows 7, Windows Server 2012 R2, Windows Server 2012, Windows 8.1, Windows Server 2016, Windows Server 2008 R2, Windows 10, Windows

Source: MITRE

Description Last Modified: 05/09/2018

First Reference

From Twitter by @DeepSightAlerts

 @deepsightalerts "Microsoft Internet Explorer Vbscript engine CVE-2018-8174 arbitrary code execution internet E-<https://t.co/2n9W5xAW7H>."

From Twitter by @DeepSightAlerts on May 8, 2018, 17:30

Resolved <https://t.co/2n9W5xAW7H> to mss.symantec.com

<https://twitter.com/DeepSightAlerts/statuses/993905875009056770> • [Reference Actions](#)

QUICK INFO

CVE Dictionary Entry:

CVE-2018-8174

NVD Published Date:

05/09/2018

NVD Published Date:

05/09/2018

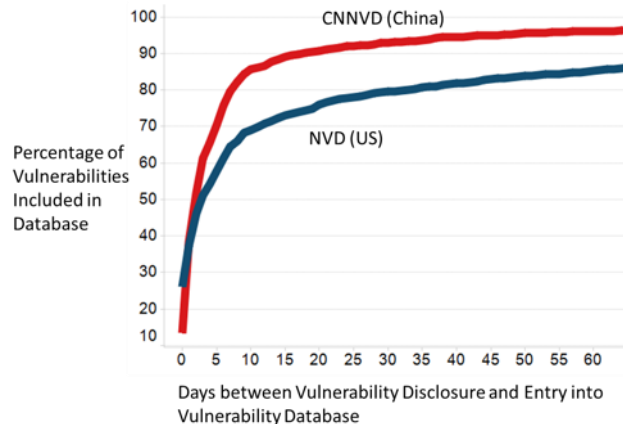
NVD Last Modified:

NVD –
Too Little, Too Late?



How fast is the process?

- CNNVD average of 13 days for publication
- US-NVD takes 33 days
- 1,794 CVEs are currently in CNNVD and absent in NVD
- Opportunities
 - For hackers to exploits
 - For defenders to monitor



t=0: Disclosure

t+2: CNNVD

t+20: NVD



t=0: Disclosure

t=0: CNNVD

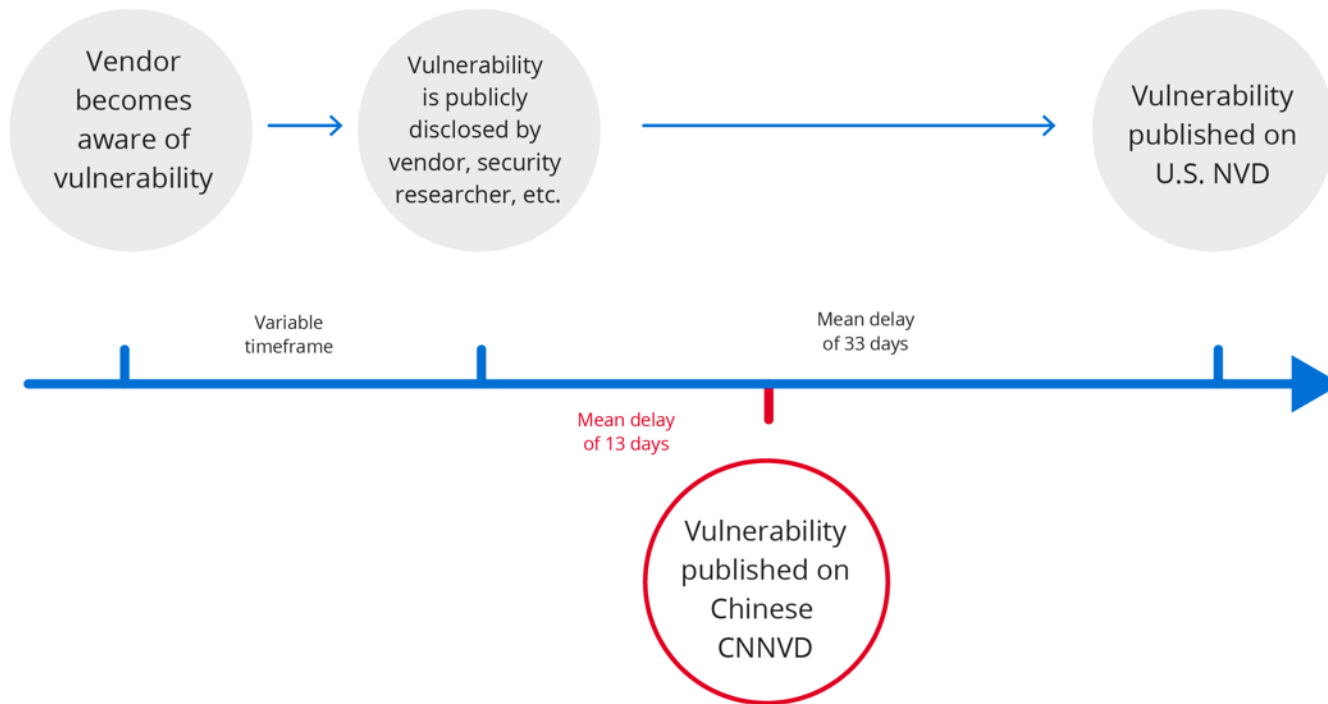
t+3: NVD

NVD –
Too Little, Too Late?



Recorded
Future

Vulnerability Reporting Timeline



NVD –
Too Little, Too Late?



Recorded
Future

The MSS & China's information security system

- The MSS has broad authority over technology and systems
- MSS administers national security reviews under the cybersecurity law, also runs China's NVD.
- MSS probably leverages information from CNNVD or national security reviews for offensive operations.



Ministry of State Security (MSS)



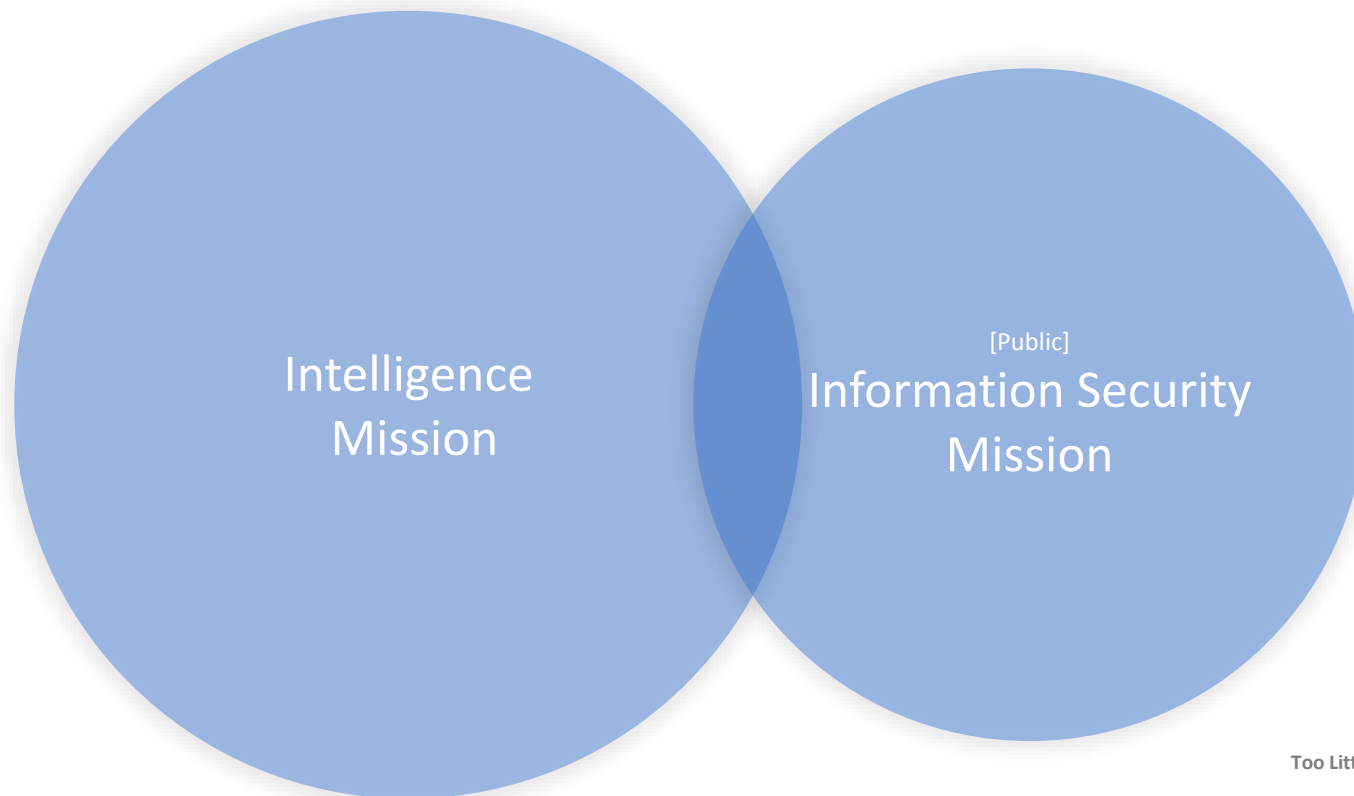
China Information Technology Security Evaluation Center (CNITSEC)



China National Vulnerability Database of Information Security (CNNVD)



CNNVD Mission?



NVD –
Too Little, Too Late?



Recorded
Future

China's Cybersecurity Law (CSL) vs GDPR

GDPR expands privacy rights of individuals

- Increases territorial scope of data privacy
- Strengthens conditions for user consent
- Companies must notify authorities of breach w/in 72 hours
- Right to be forgotten
- Establishes right of users to obtain personal data concerning them
- Privacy by design

CSL establishes state's access to any/all data

- Law standardizes collection & use of PII & requires data from Chinese users to be held in-country
- Creates two new definitions: "Network operators" and "Critical information infrastructure"
- Institutes "national security reviews", conducted by CNITSEC
- Companies are required to make recommended changes



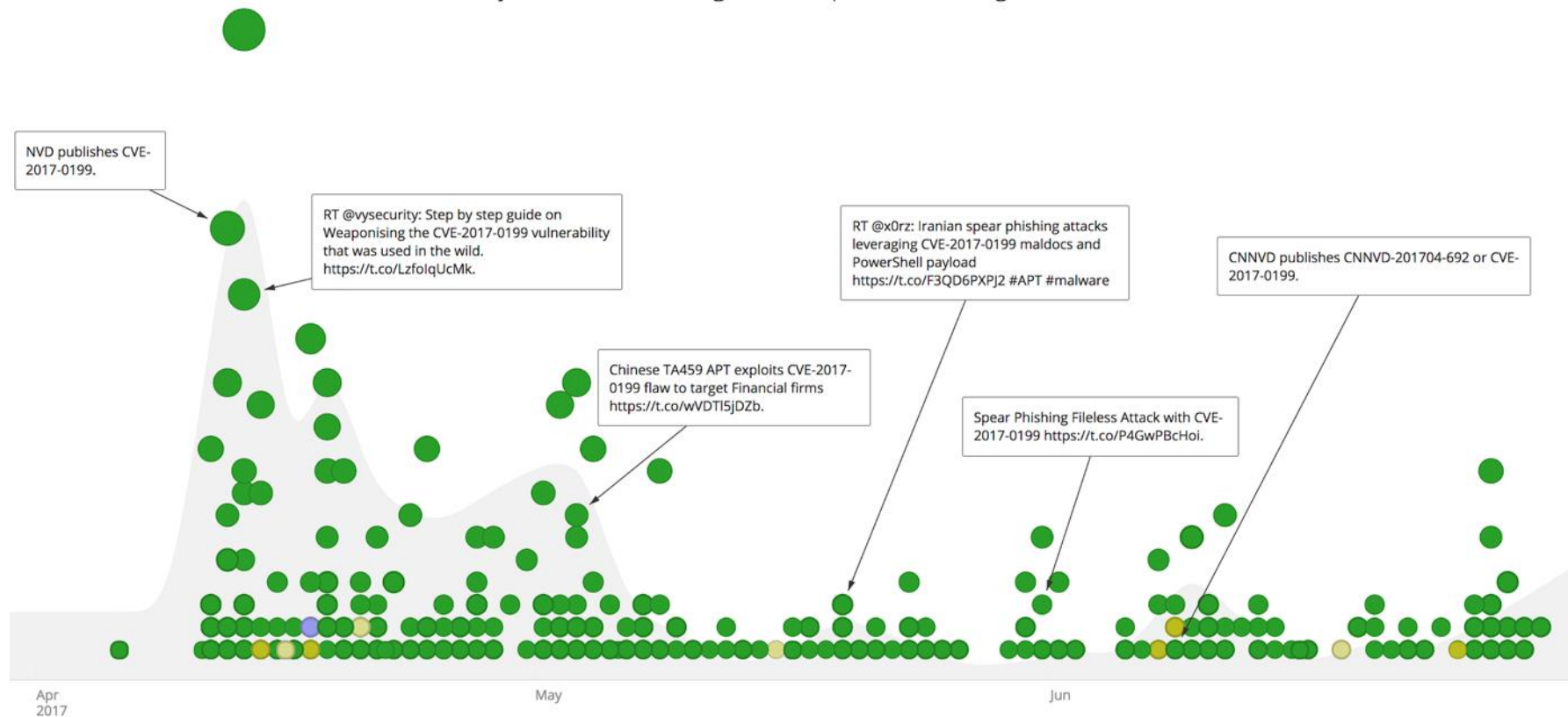
Studying Statistical Outliers Revealed...

CNNVD has a formal vulnerability evaluation process in which high-threat CVEs are likely evaluated for their operational utility by the MSS before publication.

- CNNVD is essentially a shell for the MSS; it has a webpage but appears separate from the MSS in name only.
- CNNVD takes longer to publish high threat vulnerabilities than low threat ones (another indicator of an evaluation process).
- For vulnerabilities with known exploits, NVD beats CNNVD to publication 85% of the time.
- CVE-2017-0199: Was being actively exploited by a Chinese APT group (TA459) during the CNNVD publication lag.



Timeline of cyber events during CNNVD publication lag of CVE-2017-0199



NVD –
Too Little, Too Late?



Recorded
Future

Influence of MSS: Example #2

Shanghai Adups example (CVE-2016-10136 & CVE-2016-10138)

- November 2016 New York Times reports on pre-installed backdoor on Android phones, speculates that it is being used by Chinese gov't to collect intelligence
- January 2017 published in U.S. NVD
CVSS Score of 7.2 (High)
- September 2017 published in CNNVD

Despite averaging 13 days to disclose new vulnerability, and regularly beating NVD, CNNVD takes 236 days after NVD publishes to report these two CVEs



NVD –
Too Little, Too Late?



Recorded
Future

Fast Forward Six Months!

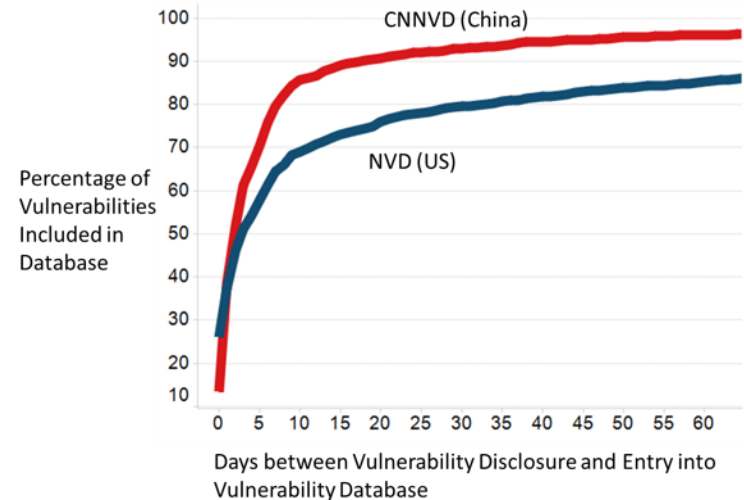
NVD –
Too Little, Too Late?



Recorded
Future

US NVD was listening

- We reviewed September 2017 Analysis with NVD officials
- Since then (6 months)
 - US-NVD average delay has dropped from 33 to 27 days
 - CNNVD average delay dropped from 13 to 12
 - NVD is catching up on the backlog
 - 1,651 CVEs are currently in CNNVD and absent in NVD
 - 1,746 CVEs were in CNNVD and absent from NVD at time of original report



NVD improved days to 75% coverage (16 vs 20 days)
NVD improved days to 90% coverage (79 vs 92 days)
CNNVD performance unchanged

NVD –
Too Little, Too Late?



Recorded
Future

- CNNVD were also listening...

没有看到这项研究

看到了研究并忽略了

看到，研究，继续前进



CNNVD were also listening...

- Instead of mitigating influence of MSS on public reporting process...
- *They tried to cover it up*
- Original report had 268 “outlier” CVEs for the prior 2 year period
- CNNVD backdated 267 of those CVEs to match or beat NVD in an attempt to:
 - Hide evidence of the vulnerability assessment process,
 - Obfuscate which vulnerabilities the MSS may be utilizing in offensive operations,
 - Limit what methods researchers can use to anticipate Chinese APT behaviour.



5 KEY TAKE AWAYS

NVD –
Too Little, Too Late?



Recorded
Future

5 KEY TAKE AWAYS

- Vulnerability management is an important part of security management
- NVD is surprisingly slow in updating information
- CNNVD is often faster than NVD, but not in all cases, and slowness correlates with Chinese use of vulnerabilities
- CNNVD manipulation of dates indicates it is controlled by MSS
- Only tracking the official NVD site is not enough – information about new vulnerabilities leaks in other channels before becoming visible in NVD

Thanks for listening!

truve@recordedfuture.com

@truve

+46705933885