cyr3con®
be in the know, now.

SIP IoT社会に対応したサイバー・フィジカル・セキュリティ
ONLINEシンポジウム2020

ハッカーを先回り：
ソフトウエアのサプライチェーンの次の攻撃と問題点を予測する

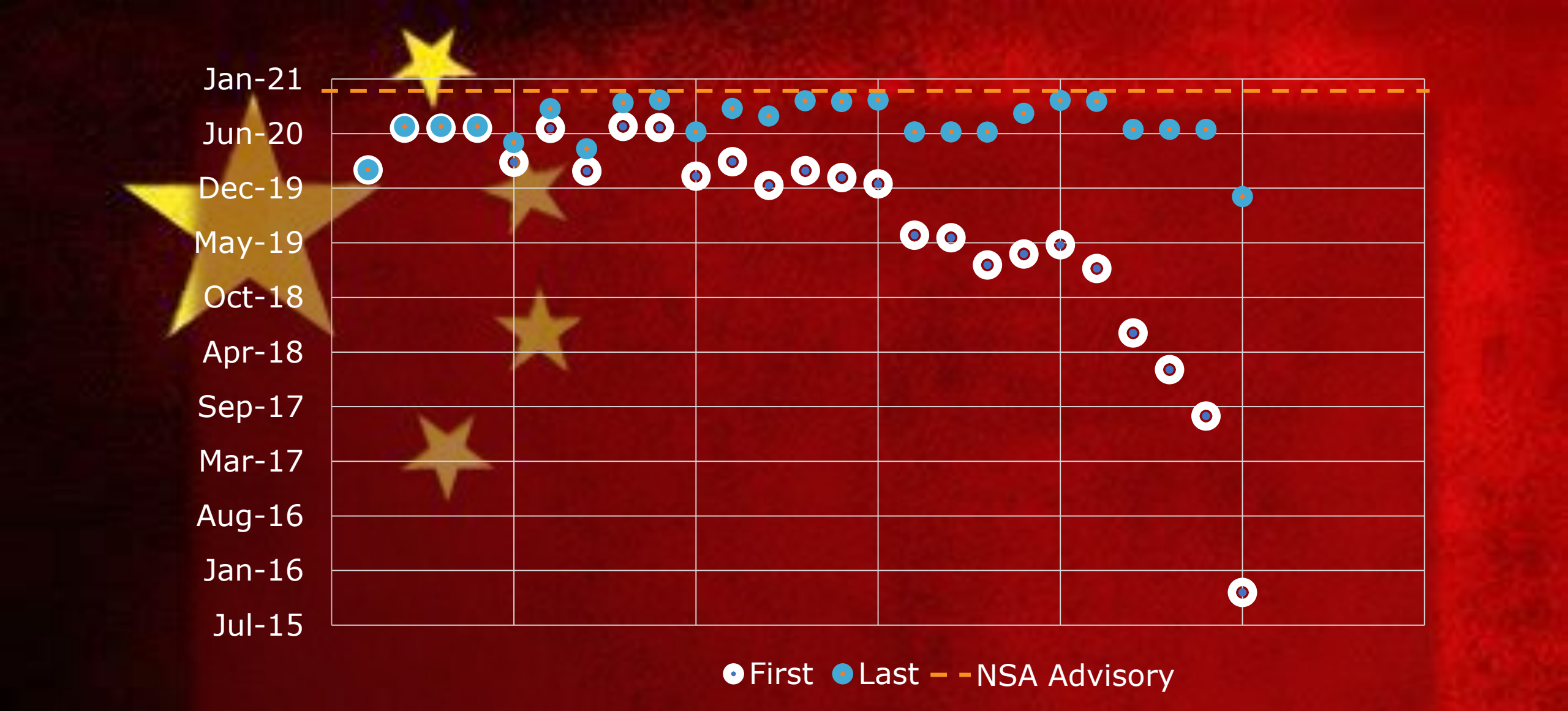
Getting ahead of hackers:
Predicting the next exploit and ramifications for the software supply chain

Paulo Shakarian, Ph.D.
CEO, CYR3CON


An October 2020 NSA advisory listed vulnerabilities exploited by Chinese government hackers.


An October 2020 NSA advisory listed vulnerabilities exploited by Chinese government hackers.
44% of the vulnerabilities are non-critical by all current security tools.


An October 2020 NSA advisory listed vulnerabilities exploited by Chinese government hackers.
44% of the vulnerabilities are non-critical by all current security tools.
Yet hackers discussed them prior to the NSA advisory.

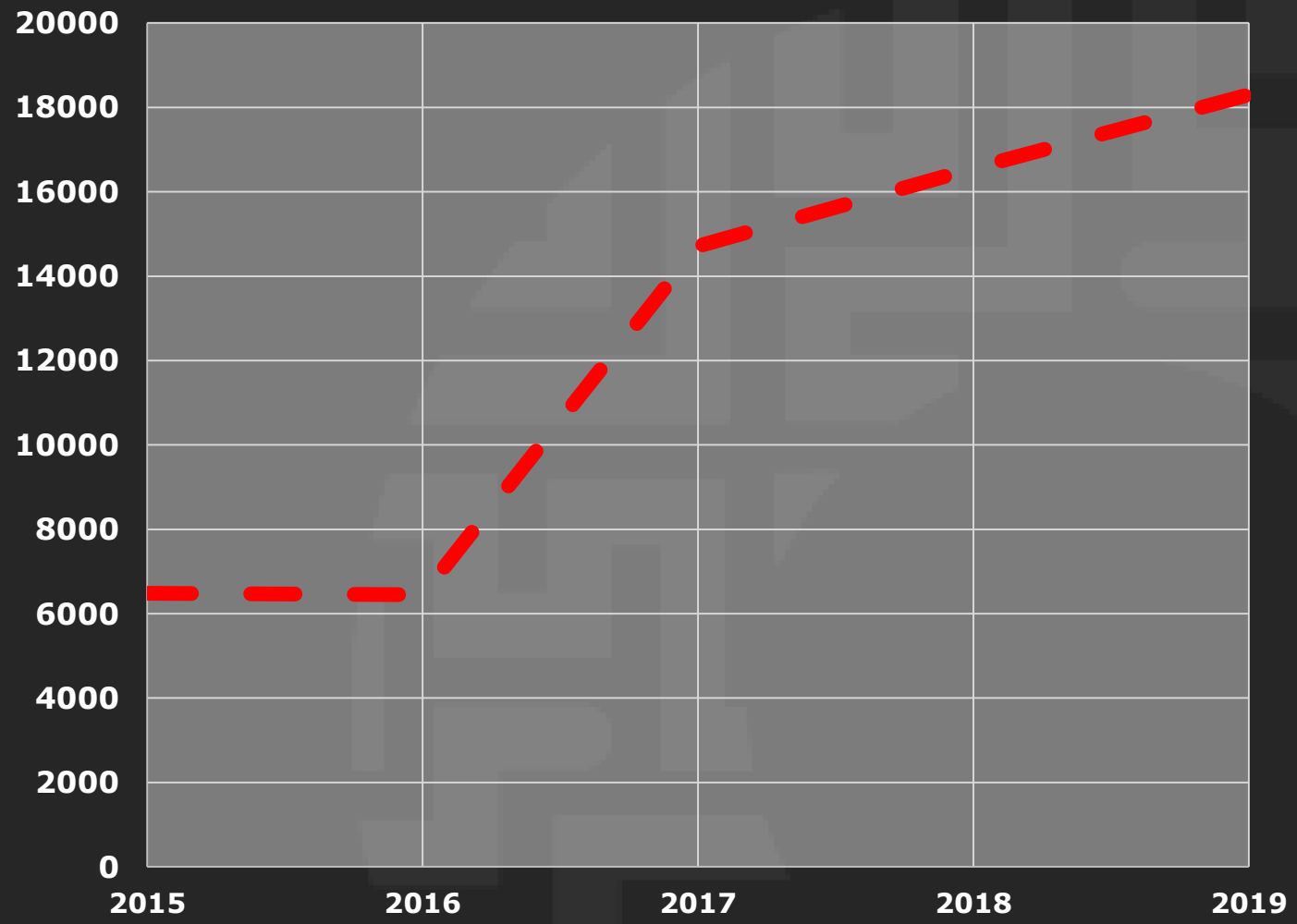


Hacker discussions prior to the NSA Advisory.

There are millions of hacker posts each month.

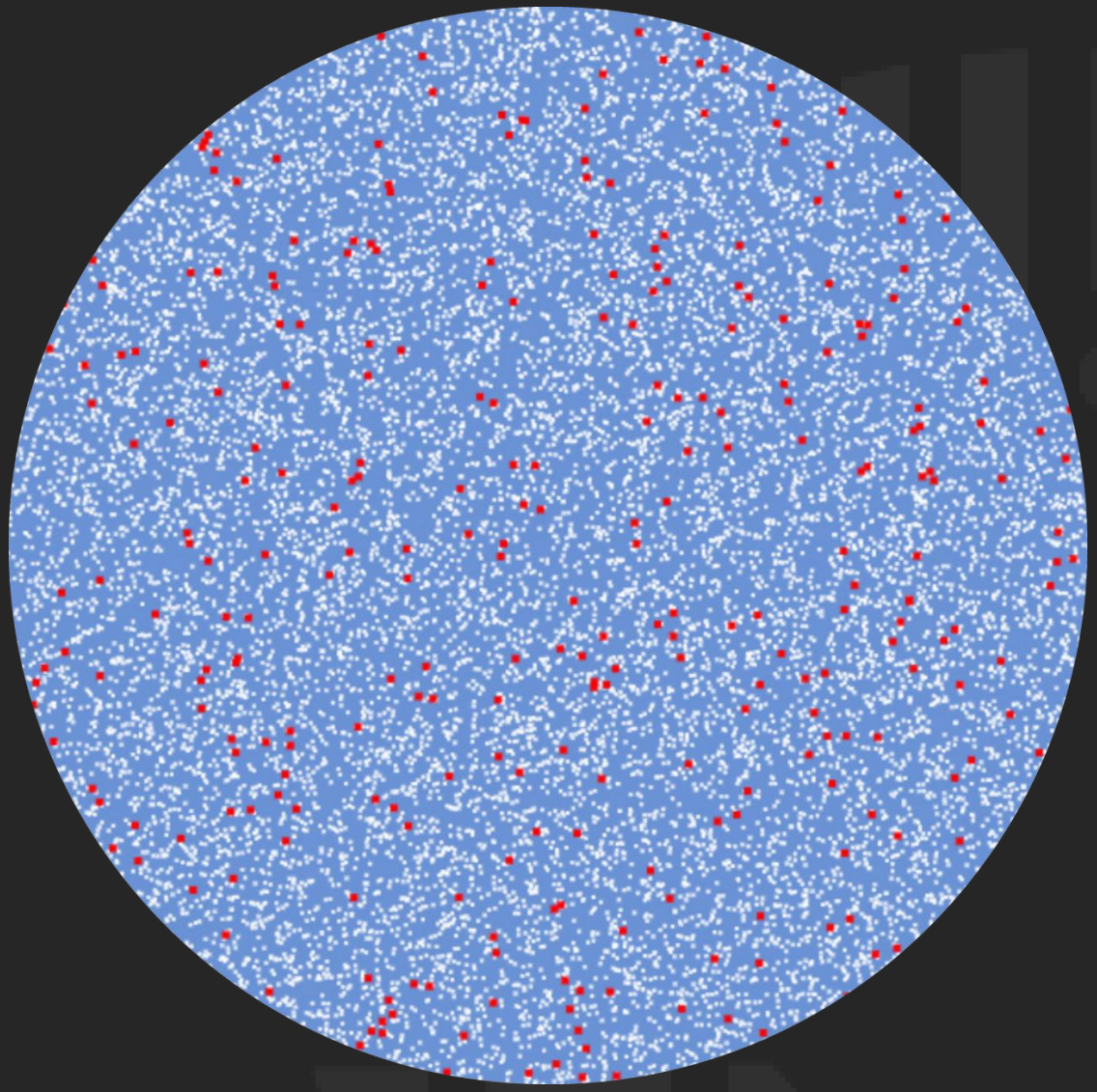
cyr3con™ be in the know, now.

There are over 1,000 software vulnerability disclosures each month.



cyr3con
be in the know, now.

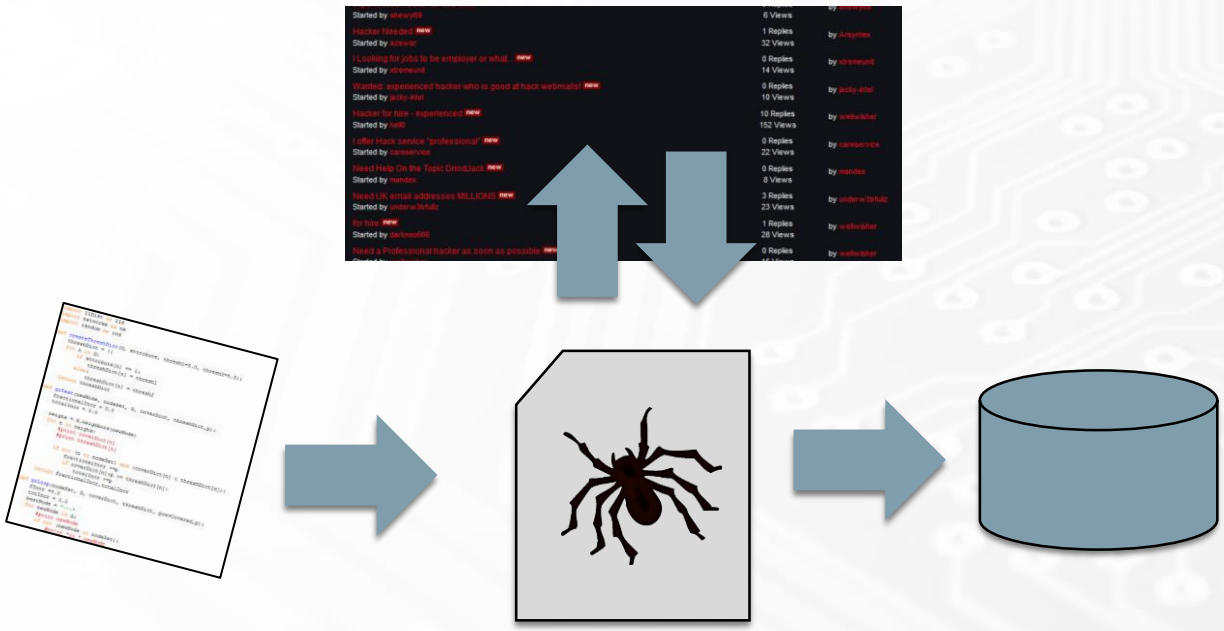
But hackers use less than 3% of vulnerabilities. How can we predict?



In 2015, the U.S. Office of Naval Research funded a machine-learning based project to predict hacker actions.

Automated Collection at Scale

CYR3CON infrastructure collects hacker discussions at scale.



Social media, deepweb, darkweb, chan sites, paste sites, OSINT, security websites, repositories, etc.

1,000+ sources

Millions of OSINT pages per day

170,000+ deepweb/ darkweb posts per day

80,000+ social media posts per day

CYR3CON-owned data collection.
Data collected by 100% legal means.
Existing European customers.

cyr3con be in the know, now.

Highly Accurate Machine Learning

MULTIPLE INDICATORS

- Hacker Social Structure
- Content of hacker Discussions
- Hacker Community Metadata
- Technical Information

MACHINE LEARNING

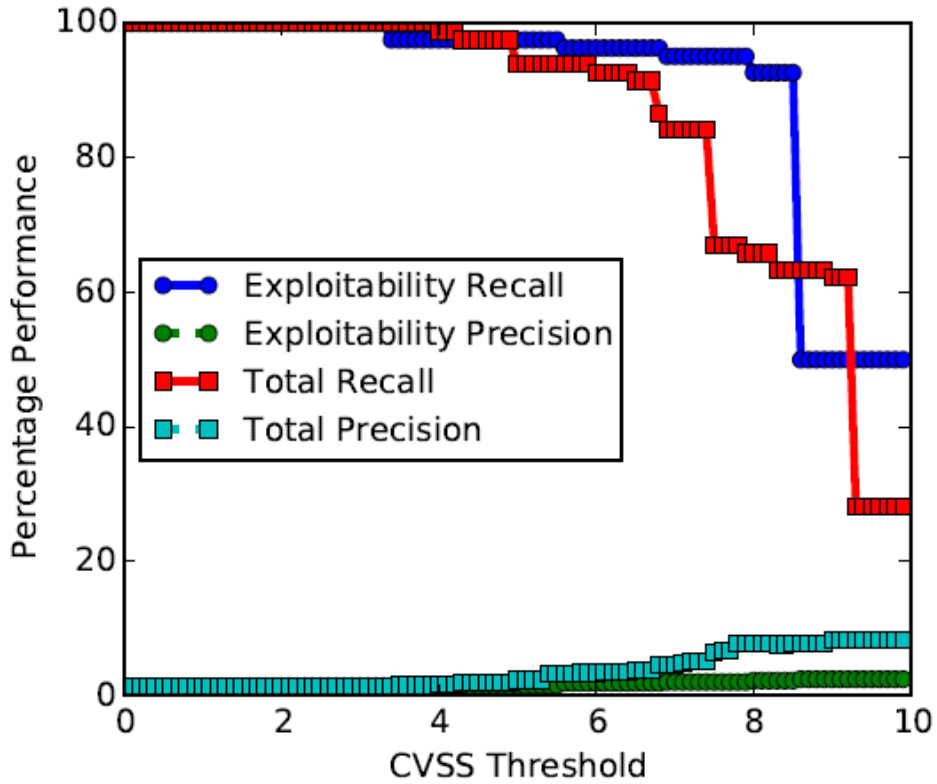
- Patented Hacker Knowledge Graph Powered Features
- Proprietary Blend of Over 60 Parallelized Models
- Computed Probability of Exploitation

WORKFLOW

- Vulnerability Management
- Patch Management
- Cloud & Dev Sec Ops

cyr3con be in the know, now.

CVSS Scoring **is not** Predictive



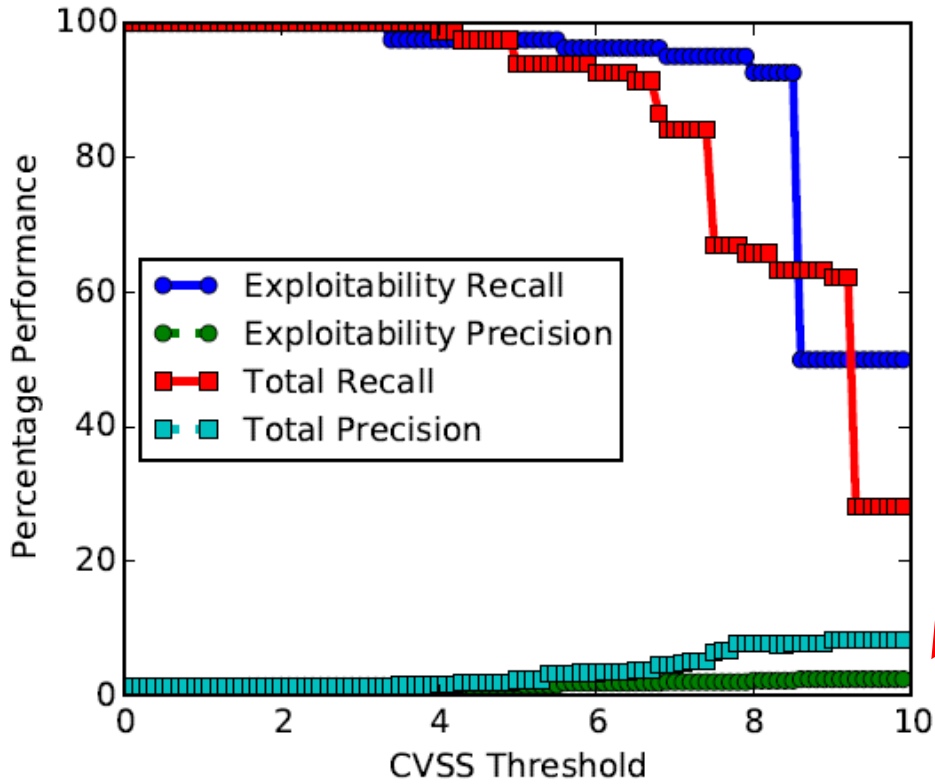
About the same as random guess

Poor performance persists - even when combined with machine learning

Holds for CVSS versions 2.0 and 3.0

Almukaynizi, M., Nunes, E., Dharaiya, K., Senguttuvan, M., Shakarian, J., & Shakarian, P. (2017, November). Proactive identification of exploits in the wild through vulnerability mentions online. In Cyber Conflict (CyCon US), 2017 International Conference on (pp. 82-88). IEEE.

CVSS Scoring **is not** Predictive



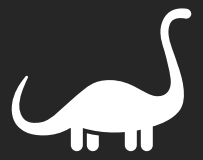
True positive rate on exploited vulnerabilities

About the same as random guess

Poor performance persists - even when combined with machine learning

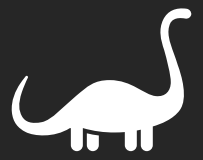
Holds for CVSS versions 2.0 and 3.0

Almukaynizi, M., Nunes, E., Dharaiya, K., Senguttuvan, M., Shakarian, J., & Shakarian, P. (2017, November). Proactive identification of exploits in the wild through vulnerability mentions online. In Cyber Conflict (CyCon US), 2017 International Conference on (pp. 82-88). IEEE.



Identify when we should upgrade legacy systems

Expensive upgrades are often avoided – which creates risk.

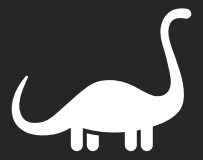


Identify when we should upgrade legacy systems

Expensive upgrades are often avoided – which creates risk.

Identify when software components will be exploited

Understand the threats to the software supply chain.



Identify when we should upgrade legacy systems

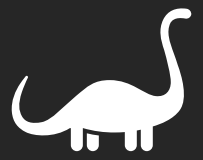
Expensive upgrades are often avoided – which creates risk.

Identify when software components will be exploited

Understand the threats to the software supply chain.

Identify threats to embedded systems (routers, IoT)

This may lead to replacement or firmware upgrades.



Identify when we should upgrade legacy systems

Expensive upgrades are often avoided – which creates risk.

Identify when software components will be exploited

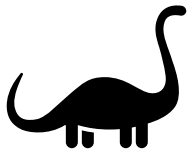
Understand the threats to the software supply chain.

Identify threats to embedded systems (routers, IoT)

This may lead to replacement or firmware upgrades.

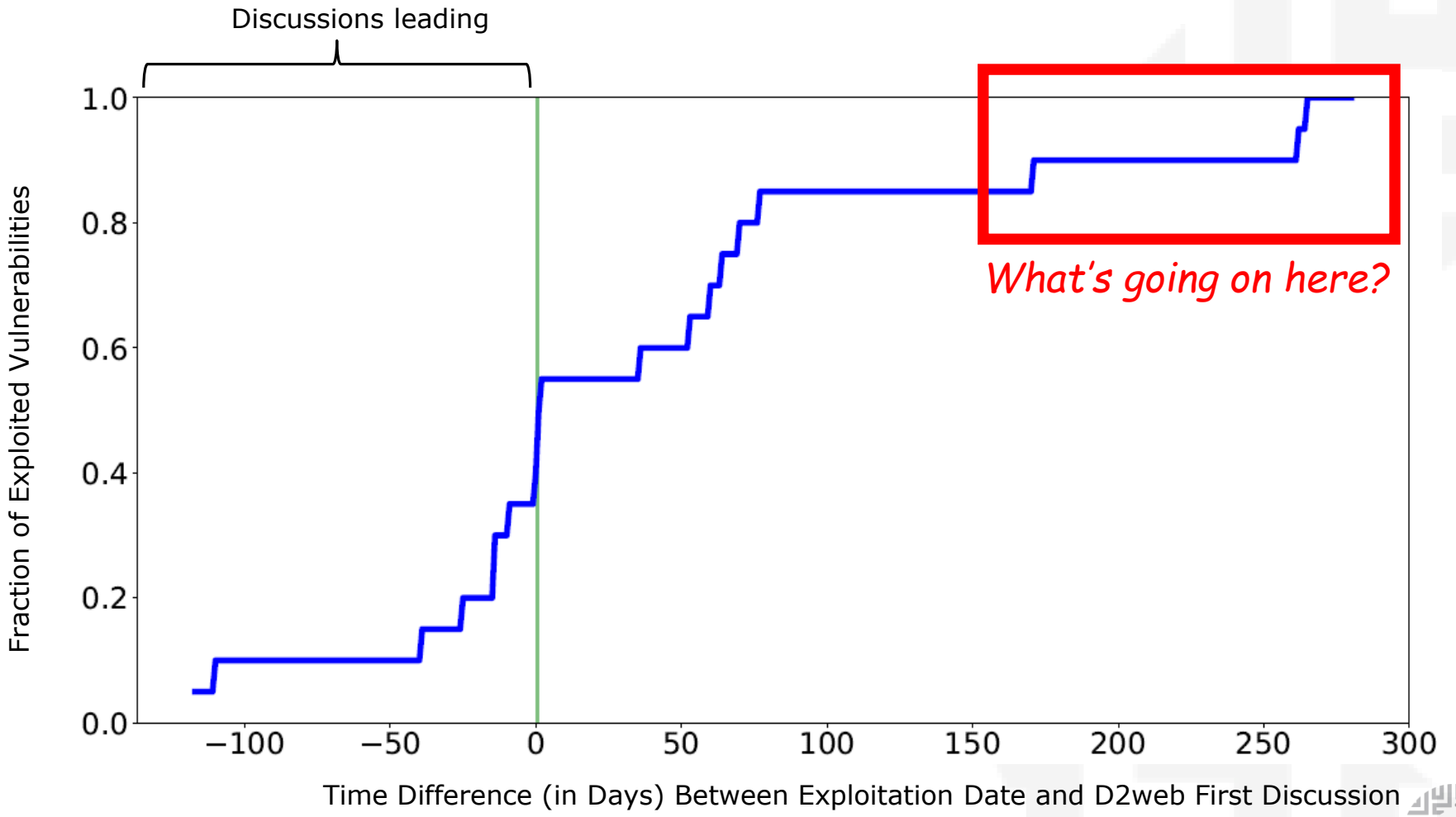
Protect work-from-home infrastructure

Cloud and VPN infrastructure has become a key enabler of pandemic-era work.



Identify when we should upgrade legacy systems

Expensive upgrades are often avoided – which creates risk.



Almukaynizi, M., Nunes, E., Dharaiya, K., Senguttuvan, M., Shakarian, J., & Shakarian, P. (2017, November). Proactive identification of exploits in the wild through vulnerability mentions online. In Cyber Conflict (CyCon US), 2017 International Conference on (pp. 82-88). IEEE.

Case Study

CVE-2018-5407 Detail

MODIFIED

This vulnerability has been modified since it was last analyzed by the NVD. It is awaiting reanalysis which may result in further changes to the information provided.

Current Description

Simultaneous Multi-threading (SMT) in processors can enable local users to exploit software vulnerable to timing attacks via a side-channel timing attack on 'port contention'.

+View Analysis Description

Severity

CVSS Version 3.x | CVSS Version 2.0

CVSS 2.0 Severity and Metrics:

NIST: NVD **Base Score:** 1.9 LOW **Vector:** (AV:L/AC:M/Au:N/C:P/I:N/A:N)

NVD Analysts use publicly available information to associate vector strings and CVSS scores. We also display any CVSS information provided within the CVE List from the CNA.

Note: NVD Analysts have published a CVSS score for this CVE based on publicly available information at the time of analysis. The CNA has not provided a score within the CVE List.

2018 vulnerability

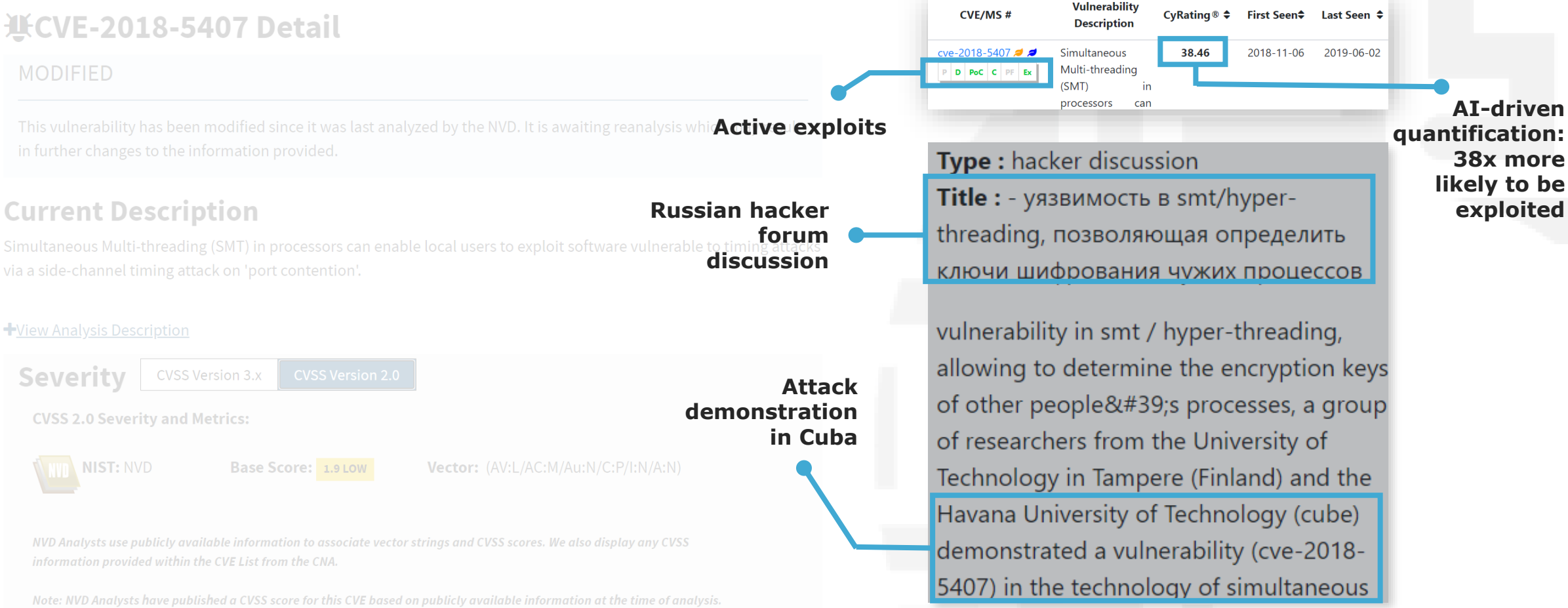
In environment of a F100 financial as of May 2020

Enterprise aware of the vulnerability

Low NIST score

cyr3con be in the know, now.

Case Study



CVE/MS #	Vulnerability Description	CyRating®	First Seen	Last Seen
cve-2018-5407 P D PoC C PF Ex	Simultaneous Multi-threading (SMT) in processors can	38.46	2018-11-06	2019-06-02

Active exploits

AI-driven quantification: 38x more likely to be exploited

Russian hacker forum discussion

Type : hacker discussion

Title : - уязвимость в smt/hyper-threading, позволяющая определить ключи шифрования чужих процессов

vulnerability in smt / hyper-threading, allowing to determine the encryption keys of other people's processes, a group of researchers from the University of Technology in Tampere (Finland) and the Havana University of Technology (cube) demonstrated a vulnerability (cve-2018-5407) in the technology of simultaneous

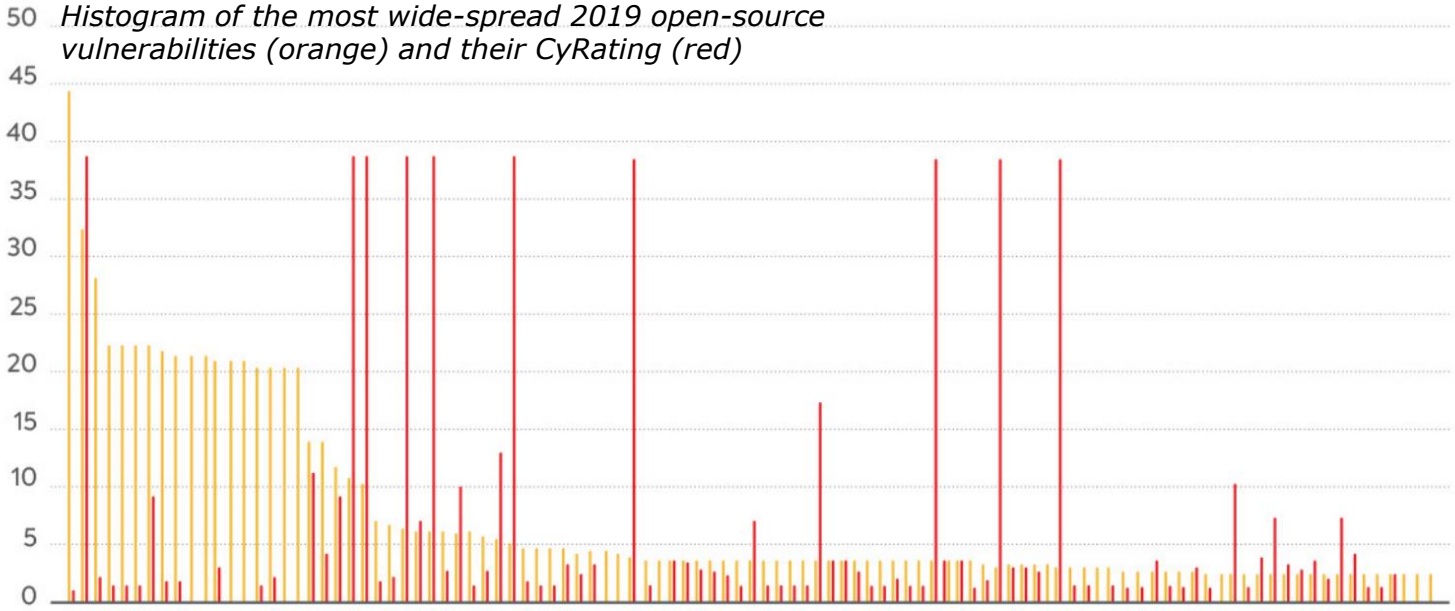
Attack demonstration in Cuba

cyr3con be in the know, now.

Identify when software components will be exploited

Understand the threats to the software supply chain.

Hackers actively target open source software an platforms.



Histogram of the most wide-spread 2019 open-source vulnerabilities (orange) and their CyRating (red)

cyr3con™ be in the know, now.

Predicted of Exploits Used in the Equifax Breach

7 March 2017

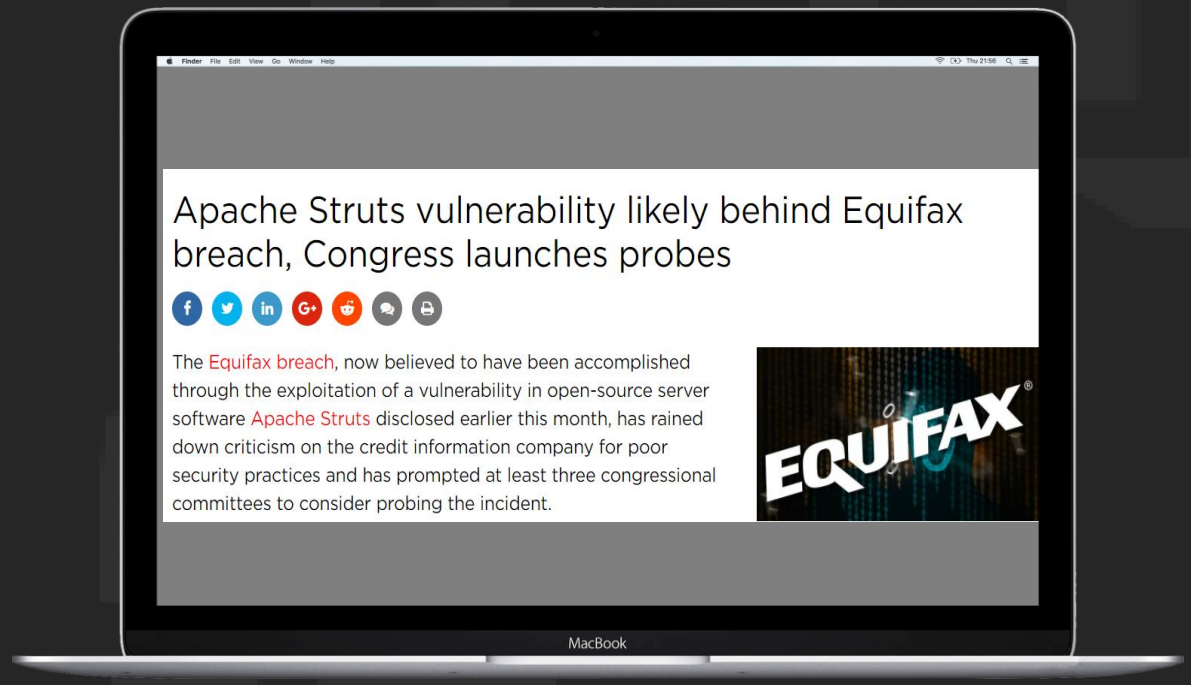
Initial machine learning assessment predicted vulnerability to be over ***10*** times more likely to be exploited than average

21 March 2017

Revised assessment had the vulnerability at over ***25*** times more likely to be exploited than average

13 May 2017

Equifax breach OCCURS

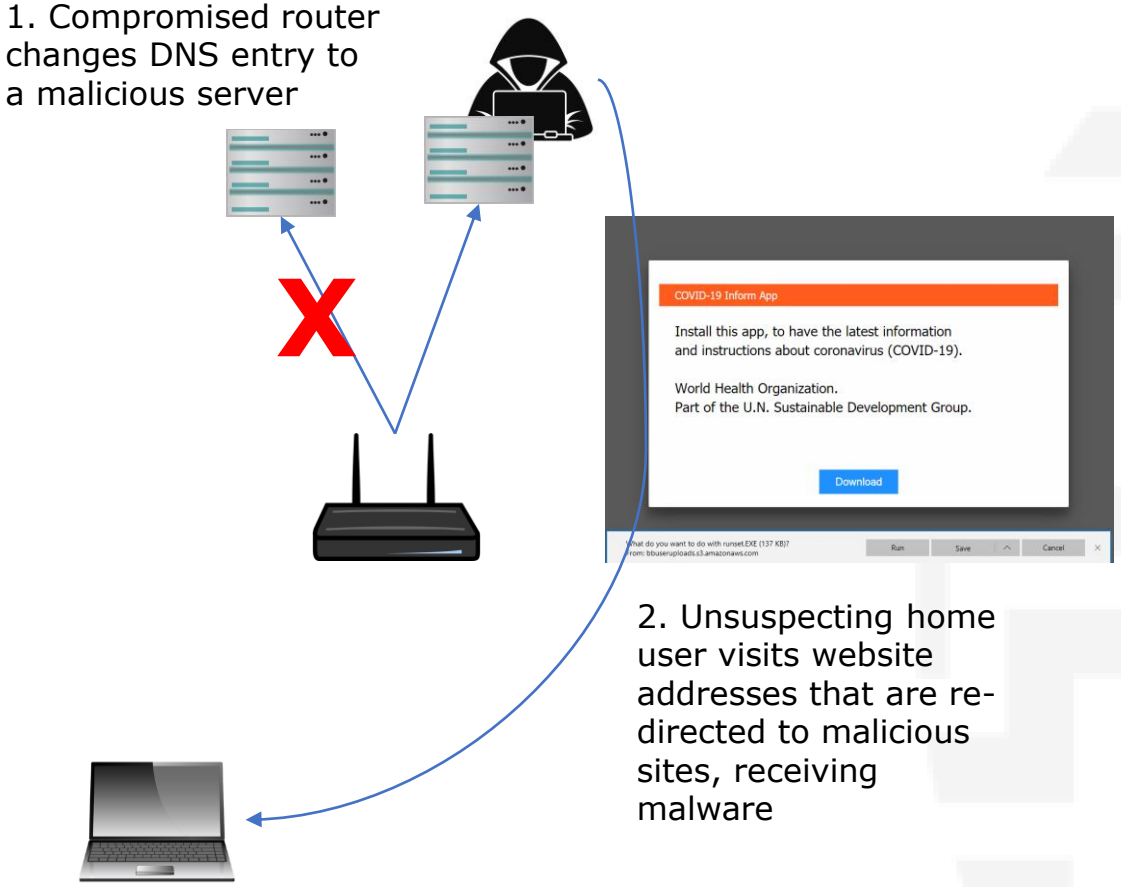


cyr3con be in the know, now.

Identify threats to embedded systems (routers, IoT)

This may lead to replacement or firmware upgrades.

This diagram outlines the Russian cyberattacks in March, 2020 that leveraged compromised routers.



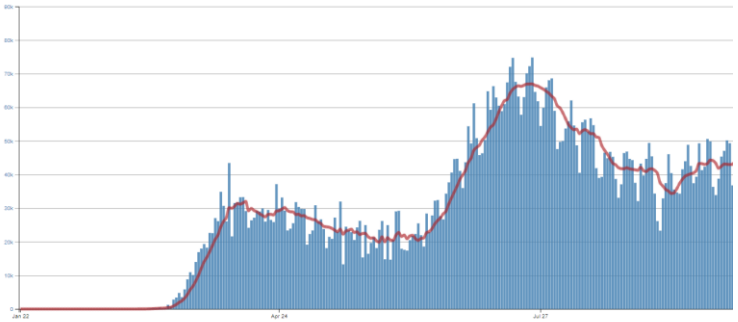
Router attacks are insidious, as enterprises have to-date been unable to trace attacks to the home router, as it has been outside of their visibility.

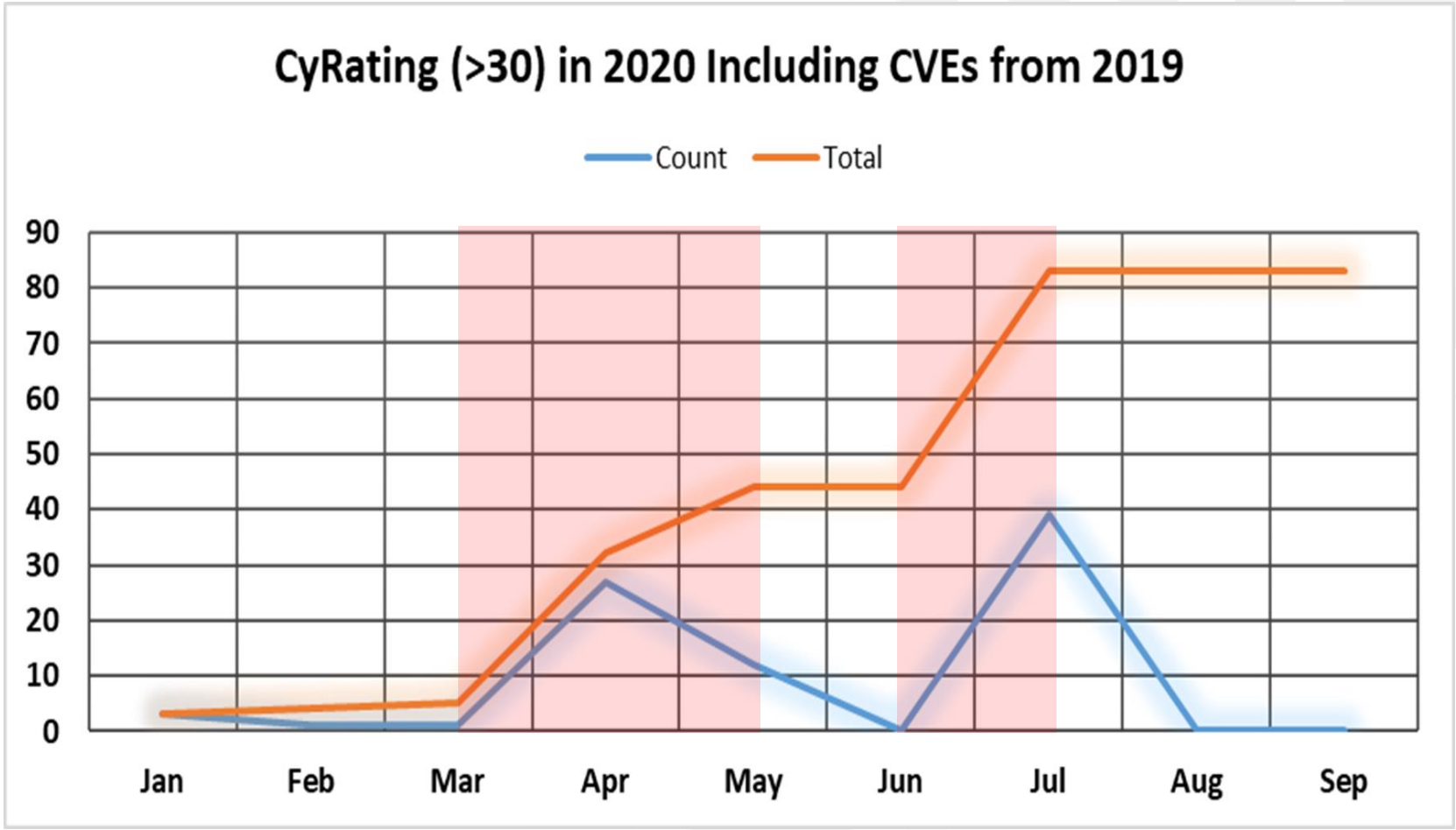
The router compromise leads to infected remote workstations as the next step of the attack. Obfuscating the source.

Router infections have risen since the pandemic started. Corporate attacks have risen as well.

Increased Hacker Interest in Router Vulnerabilities During the Pandemic

Spikes in hacker interest in home router vulnerabilities spiked during periods of time where COIVD-19 cases in the U.S. spiked. (US CDC case count in lower-left)





cyr3con be in the know, now.

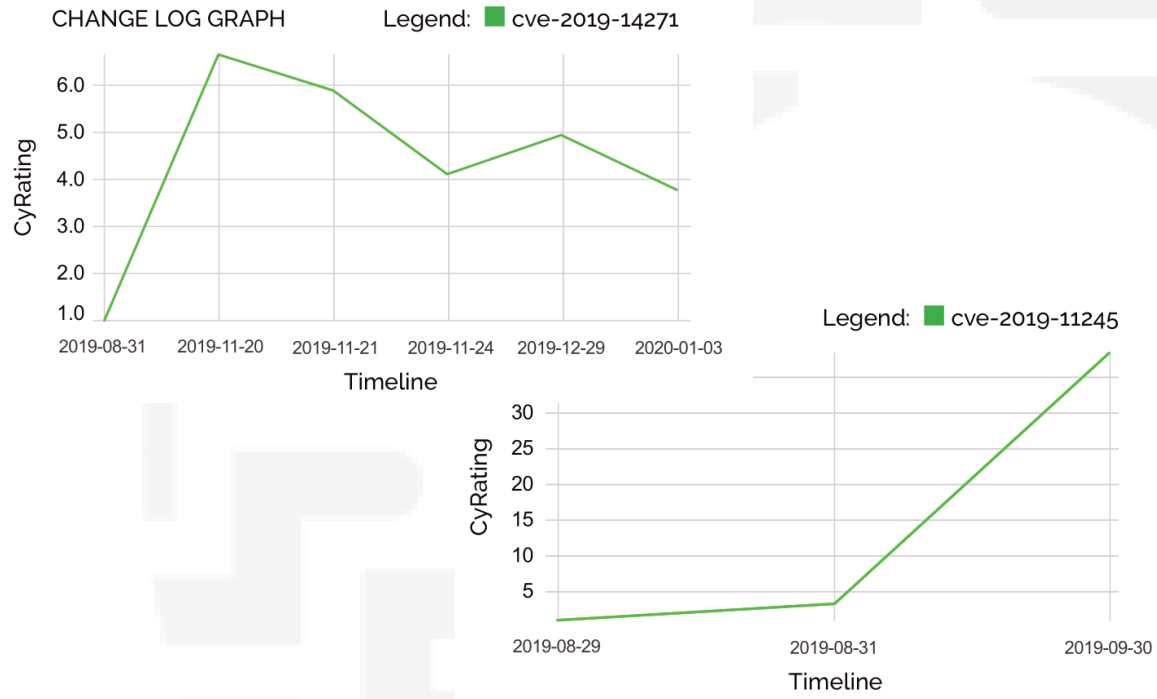
Protect work-from-home infrastructure

Cloud and VPN infrastructure has become a key enabler of pandemic-era work.

Cloud infrastructure is becoming a focal point of hackers.

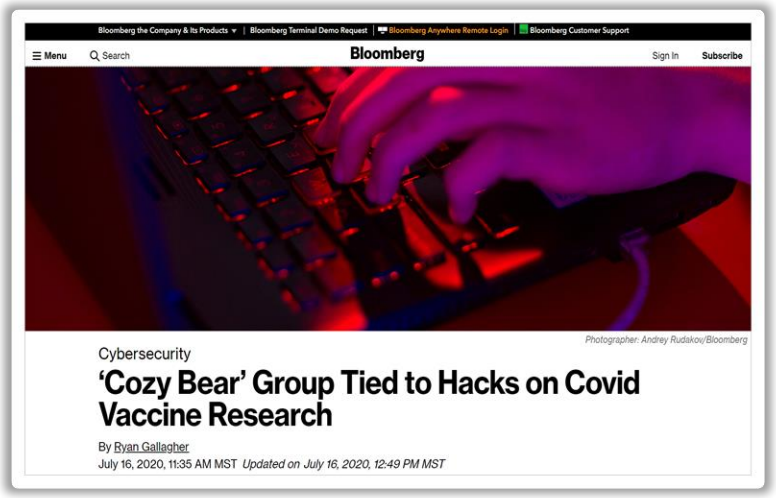
Kubernetes and Docker infrastructure are of particular interest.

CYR3CON's threat-intelligence driven CyRating for Docker vulnerability CVE-2019-14271 and Kubernetes vulnerability CVE-2019-11245 as they change over time.



cyr3con™ be in the know, now.

VPN Case Study: CozyBear and COVID-19 Research


Bloomberg the Company & Its Products | Bloomberg Terminal Demo Request | Bloomberg Anywhere Remote Login | Bloomberg Customer Support

Menu Search **Bloomberg** Sign In Subscribe

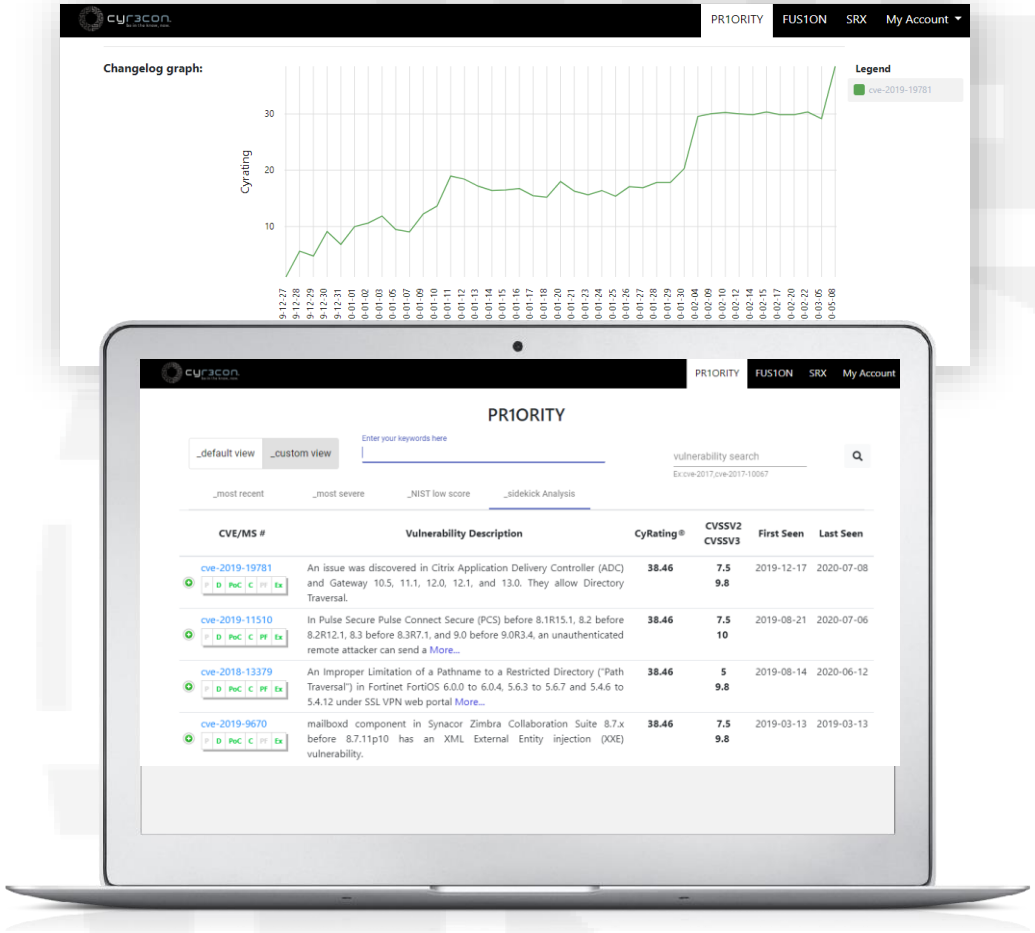
Photographer: Andrey Rudakov/Bloomberg

Cybersecurity

'Cozy Bear' Group Tied to Hacks on Covid Vaccine Research

By Ryan Gallagher

July 16, 2020, 11:35 AM MST *Updated on July 16, 2020, 12:49 PM MST*



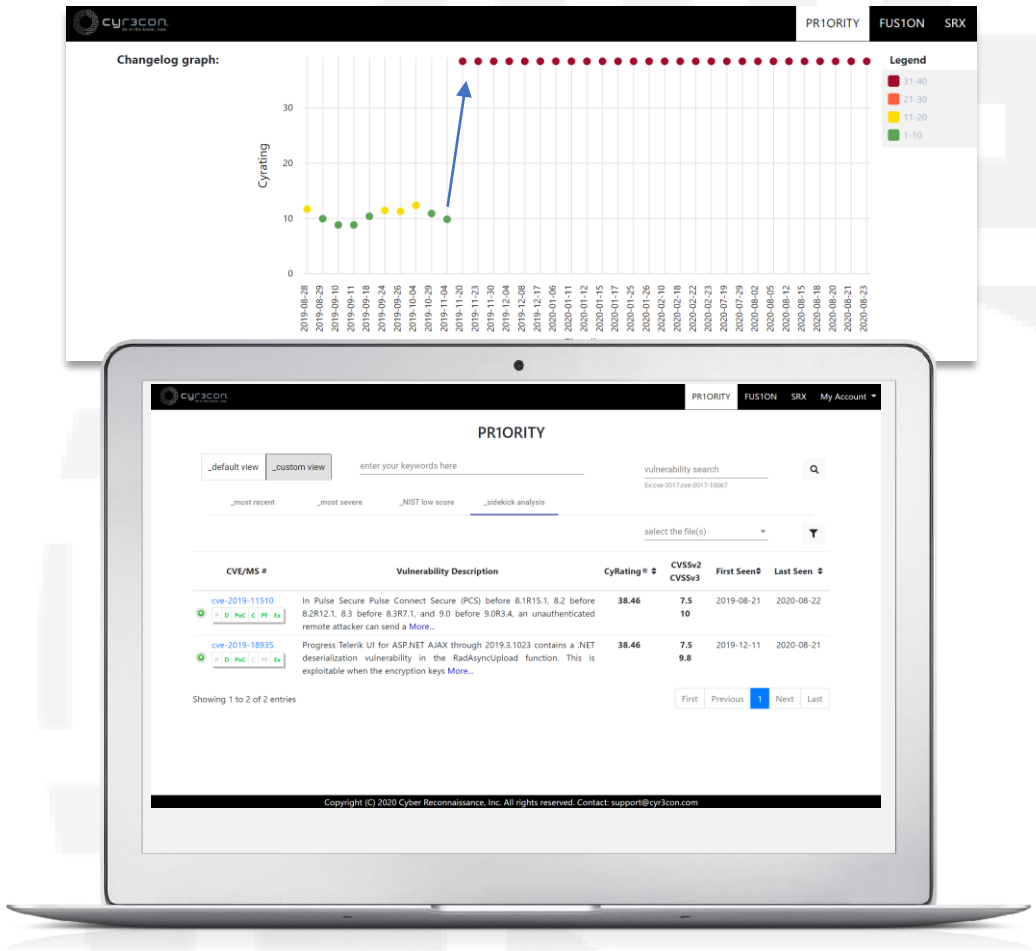
In July, 2020, Russian hacking Group, CozyBear is actively exploiting exploiting multiple vulnerabilities to steal US and UK COVID-19 related research data.

All were predicted by CYR3CON in 2019

Screenshots at the right show CYR3CON predicted exploitation of the vulnerabilities prior to this attack.

cyr3con™ be in the know, now.

VPN Case Study: NetWalker Ransomware

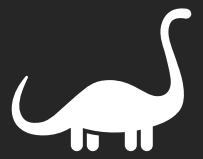


In August, 2020, the University of Utah paid hackers $457,000 due to a ransomware attack.

The vulnerabilities used by the hackers were predicted by CYR3CON month prior to the attack

Screenshots at the right show CYR3CON predicted exploitation of the vulnerabilities prior to this attack.

cyr3con be in the know, now.



Identify when we should upgrade legacy systems

Expensive upgrades are often avoided – which creates risk.

Identify when software components will be exploited

Understand the threats to the software supply chain.

Identify threats to embedded systems (routers, IoT)

This may lead to replacement or firmware upgrades.

Protect work-from-home infrastructure

Cloud and VPN infrastructure has become a key enabler of pandemic-era work.

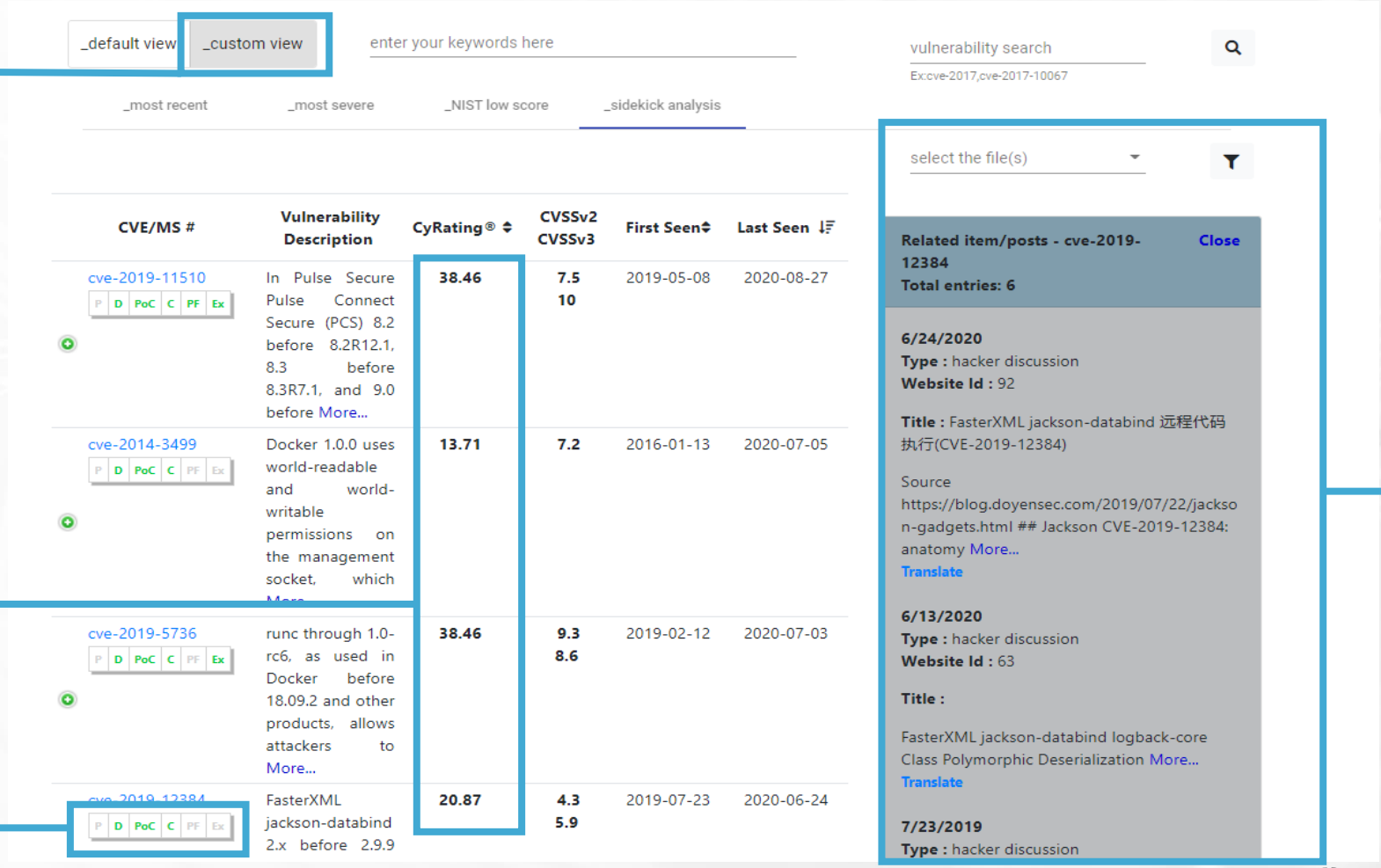
CYR3ON PR1ORITY:

The World's First Cyber Prediction Platform using AI

Customizable dashboards and workflow integrations enable environment-specific predictions

Timely and accurate quantified predictions

Aggregated metadata



Contextual Prediction provides the intelligence that drove the prediction

cyr3con be in the know, now.

ありがとうございました
Thank You

Visit https://www.change-jp.com/ for more information.

CHANGE

PEOPLE, BUSINESS, JAPAN

cyr3con®
be in the know, now.

SIP IoT社会に対応したサイバー・フィジカル・セキュリティ
ONLINEシンポジウム2020

ハッカーを先回り：
ソフトウエアのサプライチェーンの次の攻撃と問題点を予測する

Getting ahead of hackers:
Predicting the next exploit and ramifications for the software supply chain

Paulo Shakarian, Ph.D.
CEO, CYR3CON