

# RSA® Conference 2022

San Francisco & Digital | June 6 – 9

SESSION ID: HTA-W09

## State of the Hack: NSA's Perspectives

Rob Joyce, NSA Cybersecurity Director

@NSA\_CSDirector

# TRANSFORM



# RUSSIA-UKRAINE



# Timeline of Russian Malicious Cyber Activity

JANUARY

**13-14 | Ukrainian Websites Defaced**

**15 | Microsoft reveals discovery of malware in Ukrainian Websites**

**16 | Ukraine blames Russia for attack on Ukrainian websites**

**18 | Data wiped at Ukrainian government agencies**

JANUARY

FEBRUARY

**15 | Ukraine's defense ministry hit by DDoS attack**

**23 | New form of destructive malware discovered in Ukrainian networks**

**Ukrainian banking and government websites hit by DDoS attack**

**24 | Viasat cyberattack impacts broadband service in Ukraine and across Europe**





# PEOPLE'S REPUBLIC OF CHINA



# EXPOSING THE THREAT

**CPO MAGAZINE** HOME NEWS INSIGHTS RESOURCES

**CYBER SECURITY** NEWS · 5 MIN READ

## NSA Publishes List of 25 Top Vulnerabilities Exploited by Chinese Hackers; Beijing Calls Us an "Empire of Hacking" in Response

ALICIA HOPE · OCTOBER 29, 2020

## DARKReading

The Edge DR Tech Sections Events

Threat Intelligence | 2 MIN READ | ARTICLE

## NSA Reveals the Top 25 Vulnerabilities Exploited by Chinese Nation-State Hackers

Officials urge organizations to patch the vulnerabilities most commonly scanned for, and exploited by, Chinese attackers.

Dark Reading Staff Dark Reading

October 21, 2020

The US National Security Agency (NSA) today published a list of the top 25 publicly known vulnerabilities most often scanned for and targeted by state-sponsored attackers out of China.

Dmitri Alperovitch @DALperovitch · Oct 21  
This is great work by @NSACyber and exactly the type of actionable value and detail that Cybersecurity Directorate is uniquely qualified to provide to the public. Knowing which vulnerabilities are most critical to patch due to use by adversaries is invaluable!

NSA Cyber @NSACyber · Oct 20  
Chinese state-sponsored malicious cyber actors are exploiting publicly known #vulnerabilities. Network defenders should take action to protect against this activity.

For a full list of CVEs & related mitigations review our latest #cybersecurity advisory: nsa.gov/News-Features/...

## CYBERSECURITY ADVISORY

### Chinese State-Sponsored Actors Exploit Publicly Known Vulnerabilities

NSA Cyber @NSACyber  
We collaborated with @CISAgov & @FBI on our #cybersecurity advisory, detailing Chinese state-sponsored actor #TTPs used against U.S. and allied networks. For a thorough understanding of this cyberthreat, read our overview, observed TTPs & mitigations. nsa.gov/news-features/...

7:36 AM · Jul 19, 2021 · Twitter Web App

**CYBERSCOOP**

GOVERNMENT

## US agencies circulate warning about 'aggressive' Chinese hacking effort to steal secrets from a range of targets

### US, NATO to 'expose' China for 'malicious cyber activities'

It's the first time NATO has condemned Chinese "cyber activities."

By [Justin Gomez](#)  
July 19, 2021, 2:47 PM

Share



# PRC State-Sponsored Cyber Actors Exploit Network Providers and Devices



---

## CYBERSECURITY ADVISORY

# RANSOMWARE





**OUR ADVERSARIES  
ARE IN THE CLOUD**



# LET'S LOOK AT SOME STAGGERING STATS

The public cloud service market is expected to reach **\$623.3 Billion** by 2023 worldwide

**94% of enterprises** already use a cloud service. And the other 6% don't know they're using cloud.

**30%** of all IT budgets are allocated to cloud computing.

**66% of enterprises** already have a central cloud team or a cloud center of excellence.

Organizations leverage almost **5 different cloud platforms** on average.

**50%** of enterprises spend more than **\$1.2 million** on cloud services annually.

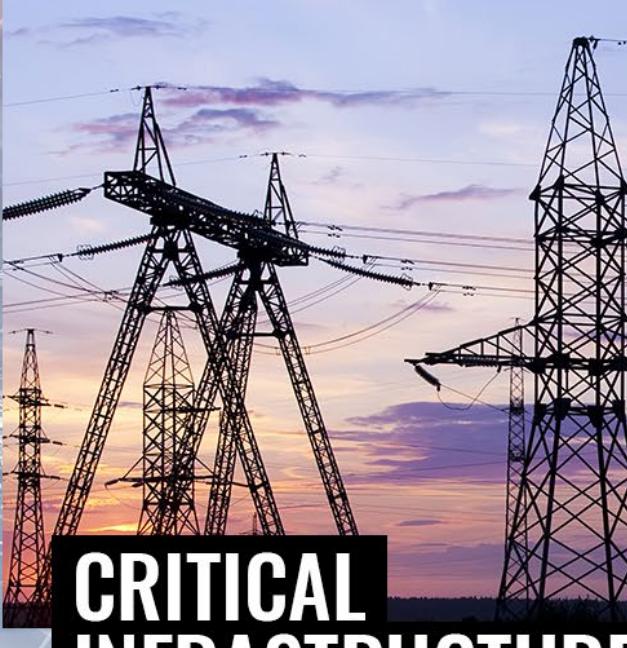
**By 2025**, the data stored in cloud data centers will **exceed 100 Zettabytes**.



# WE ALL USE IT



**PRIVATE INDUSTRY**



**CRITICAL  
INFRASTRUCTURE**



**GOVERNMENT & IC**



# SOLARWINDS



## CONDUCT OPEN SOURCE RECONNAISSANCE

The actor conducted target development via LinkedIn, Facebook, Twitter, and open source research, pulling publicly available information.

1

2

3

4

## ESTABLISH INITIAL ACCESS INTO THE TARGET NETWORK

The actor leveraged a backdoor in SolarWinds as well as other additional access vectors.

## ESCALATE PRIVILEGES

The actor escalated privileges and manipulated trust to masquerade as a legitimate user/service, degrading Office 365 security.

## CONDUCT DATA EXFILTRATION

The actor exfiltrated data through U.S. cloud service providers via encrypted data flows, hiding it in plain sight.



# NOBELIUM





A screenshot of a GitHub pull request interface showing the CI/CD status. It displays a summary message: "Some checks were not successful" with "2 failing and 2 successful checks". Below this, four successful checks are listed: "ci/your\_ci" (tests passed), "codecov/project" (35% coverage compared to 507ba38), "codecov/project/backend" (87% coverage compared to 507ba38), and "codecov/project/api" (90% coverage remains the same). At the bottom, there is a warning about conflicts: "This branch has conflicts that must be resolved. Use the command line to resolve conflicts before continuing." Buttons for "Merge Pull request" and "View on GitHub Desktop" are also visible.





# STRATEGIC COMPETITION



# NSA PRODUCTS

ESF CLOUD PAPERS

KUBERNETES  
HARDENING GUIDANCE





**LET'S TEAM UP TO  
SECURE THE CLOUD**





**3 THINGS TO  
DO  
TOMORROW**



**3 THINGS TO  
DO  
THIS YEAR**



# RSA® Conference 2022

## Thank you

[nsa.gov/cybersecurity](http://nsa.gov/cybersecurity)

Follow @NSAcyber and @NSA\_CSDirector

