Cybersecurity

Australia and the Risk of a Russian Cyber Attack: Are You Ready?

Edward Kost
updated Jun 07, 2022

Given Russia's reputation for highly-sophisticated cyberattacks, the country's invasion of Ukraine has sparked justified fears of an imminent global cyberwar.

While, for the time being, Putin's cyber efforts against Ukraine are surprisingly restrained, this may not be the case for other countries. Russia appears to be mounting a cyberattack offensive against nations that have voiced their disapproval of Ukraine's invasion through economic sanctions - a dampened fulfillment of Putin's ominous threat of punishing any country that interferes with his efforts.

> "Whoever tries to impede us, let alone create threats for our country and its people, must know that the Russian response will be immediate and lead to the consequences you have never seen in history."

> *Vladimir Putin*
> *President of Russia*

The most recent evidence of this cyber threat being exercised occurred on Tuesday, 1 March. Just days after joining the economic sanction responses of its Western allies, Toyota was forced to halt all plant operations in Japan following a suspected supply chain attack. While Russia hasn't officially claimed responsibility, its involvement can be inferred from the sinister remarks of Mikhail Yurlevich Galuzin, the Russian ambassador to Japan.

> "Should Japan impose sanctions on Russia, there would be consequences."
>
> *MIkhail Yurlevich Galuzin*
> *Russian Ambassador to Japan*

Since Australia has also implemented economic sanctions against Russia, Australian critical infrastructures and businesses are at a heightened risk of being added to Russia's cyberattack firing line.

In recognition of this, the Australian Cyber Security Center (ACSC) has issued an urgent advisory for Australian businesses to elevate their security posture.

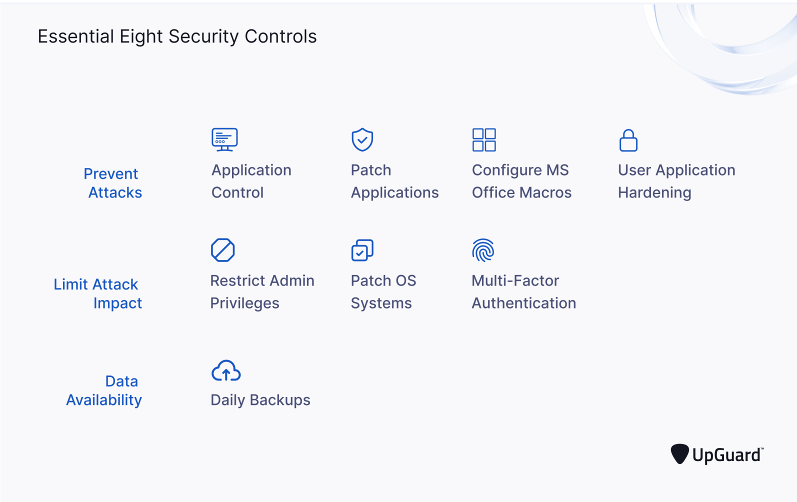
The following roadmap can help you achieve a standard of cyber resilience with the highest potential of defending against nation-state attacks.

Implement an Essential Eight Framework

According to the ACSC, the Essential Eight ensures Australian businesses meet the minimum recommended cybersecurity standard. This framework strengthens the cyber resilience of an IT network through eight strategies:

- Application control;
- Patch applications;
- Configure Microsoft Office macro settings;
- User application hardening;
- Restrict administrative privileges;
- Patch operating systems;
- Multi-factor authentication; and

Contents


Essential Eight Security Controls
Prevent Attacks
Application Control
Patch Applications
Configure MS Office Macros
User Application Hardening
Limit Attack Impact
Restrict Admin Privileges
Patch OS Systems
Multi-Factor Authentication
Data Availability
Daily Backups
UpGuard

Learn more about the Essential Eight.

Detect and Address Supply Chain Security Risks

Since January 14, 2022, Russia has launched a series of cyberattacks targeting Ukrainian government websites. Many of these attacks are believed to have been facilitated by a vulnerability in OctoberCMS, a content management solution used by the Ukrainian government.

The vulnerability tracked as CVE-2021-32648 is being used as an attack vector for a destructive new family of malware called

Author

Edward Kost

Reviewed by

Kaushik Sen

WhisperGate.

Learn more about CVE-2021-32648.

Thanks to its malevolent efficiency, the supply chain attack is a well-worn tactic in Russia's cyberattack arsenal. Instead of confronting fortified walls around common entry points, it's much simpler, instead, to slip through the backdoor by compromising a third-party vendor in a victim's supply chain.

Supply chain security risks can be instantly discovered with an attack surface monitoring solution.

The most comprehensive evaluation of the third-party threat landscape is achieved by combining attack surface monitoring with security questionnaires. Security questionnaires surface commonly overlooked third-party risks buried inside a supplier's ecosystem.

UpGuard offers a library of security questionnaires that map to popular cybersecurity frameworks, including the Essential Eight.

Click here to try UpGuard for free for 7 days.

Familiarise Yourself with Russia's Latest Malware Campaigns

Get familiar with the malware campaigns Russia is currently deploying. Each item in the list below links to a resource detailing mitigation strategies.

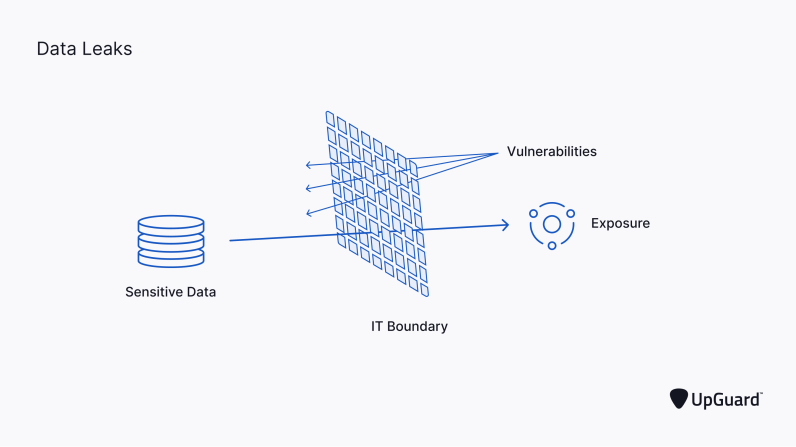
- WhisperGate
- HermeticWiper
- HermeticWizard
- IsaacWiper
- Conti Ransomware

Conti ransomware is a particularly dangerous strain of ransomware due to the speed with which it encrypts data and spreads to other systems. Fortunately, the Conti source was recently leaked by a Ukranian researcher. This invaluable intelligence could help security teams predict and intercept the Conti ransomware attack pathway.

- For more information about the lifecycle of Russia's latest destructive malware campaigns, refer to this resource by Microsoft.
- For more details about Tactics, Techniques, and Procedures (TTPS) that could be associated with Russia's malware campaigns, refer to this resource by the ACSC.
- For more information about how Australian businesses can improve their cyber resilience, visit Cyber.gov.au.

Detect and Shut Down all Data Leaks

Data leaks are overlooked exposures of sensitive data that make data breaches easier for cybercriminals. These leaks could be caused by software vulnerabilities or misconfigurations facilitating unauthorized access to sensitive resources - such as the significant Microsoft Power Apps data leak in 2021.



Like supply chain attacks, data leaks allow cybercriminals to circumvent formidable security controls by exploiting a backend vulnerability. Because of this convenience, data leak exploitation should be regarded as a probably tactic in Russia's bag of cyberattack tricks and urgently addressed.

Speed is Critical

Australian businesses need to act fast. Russia's probable cyber attack on Japan demonstrates how quickly the nation can punish those that have joined the chorus of economic sanctions.

To learn how UpGuard can help you accelerate the improvement of your security posture, get in touch with us now!

Learn more

Download our free ebooks and whitepapers

Insights on cybersecurity and vendor risk management.

View resources

Tags: Cybersecurity

See UpGuard In Action

Book a free, personalized onboarding call with one of our cybersecurity experts.

Contact sales

Free demo

Related posts

Learn more about the latest issues in cybersecurity.

Cybersecurity

The Top Cybersecurity Websites and Blogs of 2022

This is a complete guide to the best cybersecurity and information security...

Abi Tyas Tunggal
August 8, 2022

Cybersecurity

14 Cybersecurity Metrics + KPIs You Must Track in 2022

Cybersecurity metrics and key performance indicators (KPIs) are an effective way...

Abi Tyas Tunggal
August 29, 2022

Attack Surface Management

What are Security Ratings?

This is a complete guide to security ratings and common usecases. Learn...

Abi Tyas Tunggal
August 7, 2022

Cybersecurity

Why is Cybersecurity Important?

If your business isn't concerned about cybersecurity, it's only a...

Abi Tyas Tunggal
September 1, 2022

Attack Surface Management

What is Typosquatting (and How to Prevent It)

Learn about the dangers of typosquatting and what your business can do to...

Abi Tyas Tunggal
June 26, 2022

Cybersecurity

What is a Cyber Threat?

A cyber threat
(or cybersecurity threat) is the possibility of a...

Abi Tyas Tunggal
August 17, 2022

View all blog posts ›

Sign up to our newsletter

Get the latest curated cybersecurity news, breaches, events and updates in your inbox every week.

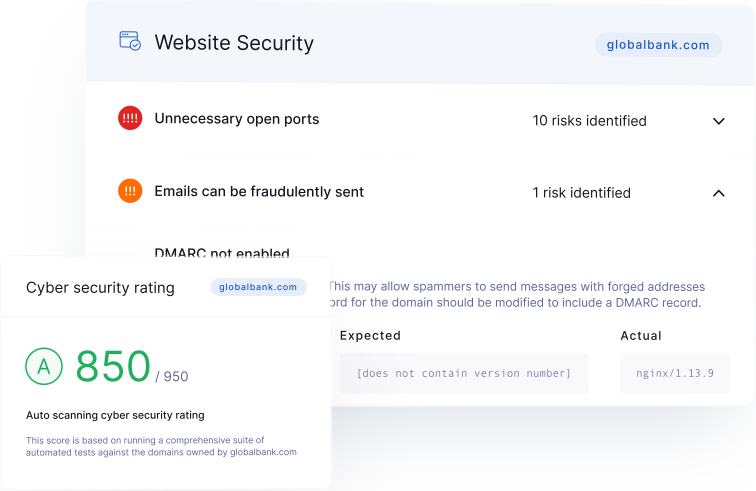
Free instant security score

How secure is your organization?

Request a free cybersecurity report to discover key risks on your website, email, network, and brand.

- ✓ Instant insights you can act on immediately
- ✓ Hundreds of risk factors including email security, SSL, DNS health, open ports and common vulnerabilities

Free score >



Website Security globalbank.com

!!!! Unnecessary open ports 10 risks identified

!!! Emails can be fraudulently sent 1 risk identified

DMARC not enabled

This may allow spammers to send messages with forged addresses
ord for the domain should be modified to include a DMARC record.

Expected: [does not contain version number]

Actual: nginx/1.13.9

Cyber security rating globalbank.com

A 850 / 950

Auto scanning cyber security rating

This score is based on running a comprehensive suite of automated tests against the domains owned by globalbank.com

UpGuard

UpGuard is a complete third-party risk and attack surface management platform.

Products

UpGuard Vendor Risk

UpGuard BreachSight

UpGuard CyberResearch

Security Ratings

Product Tour

Pricing

Release notes

Integrations

Compare

BitSight

SecurityScorecard

CyberGRX

RiskRecon

All comparisons

Solutions

Financial Services

Technology

Healthcare

Tools

Security Reports

Instant Security Score

Company

About us

Careers We're hiring!

Contact

Press

Support

Security

Insights

Events Register!

Breaches

Resources

Blog

Glossary

News

Protected by UpGuard