THREATCANARY

Advice for the CISO and Board on planning for a Cyber War

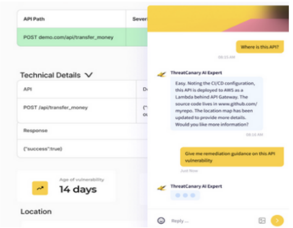
July 2024

Andrew Horton

CTO & CO-FOUNDER

- Advisor to CISOs
- Strategic rapid cyber capability uplift consulting
- Background in consulting through Security-Assessment, StratSec, BAE Systems Applied Intelligence, HackLabs, Hacktive, Mercury ISS, Path, Ayenem, HortonSec Consulting and more.
- Former Director of Engineering for CoinPayments, the world's largest cryptocurrency payments provider.
- Andrew has worked with clients in banking, telecommunications, energy, insurance, health, NGOs, & government.
- Developed security consulting services line, from pre-sales to delivery. Full-stack leader, with skills leading teams from UX design, frontend and server side development to network and server engineering.
- Andrew is best known for his open-source security research, forming part of the standard arsenal of penetration testers and black-hat hackers alike, and Kali Linux - the most popular Linux security distribution used daily by security professionals.
- Security Research in OWASP Testing Guide, Penetration Testing Execution Standard (PTES), text books like the Browser Hacker's Handbook, and much more.
- Writing the OffSec AI LLM Security Course

The Product



API Path	Sever
POST demo.com/api/transfer_money	

Technical Details

API	D
POST /api/transfer_money	{" ou
Response	
{"success":true}	

Age of vulnerability
14 days

Location

Where is this API?
08:15 AM

ThreatCanary AI Expert
Easy. Noting the CI/CD configuration, this API is deployed to AWS as a Lambda behind API Gateway. The source code lives in www.github.com/myrepo. The location map has been updated to provide more details. Would you like more information?
08:16 AM

Give me remediation guidance on this API vulnerability
Just Now

ThreatCanary AI Expert

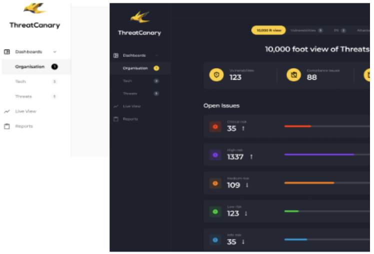
Block Data Breaches as they happen

AI Advisors for guided remediation

Complex multi-cloud and hybrid environments

Good UX with **Light** and **Dark** UI modes

Nearly zero configuration



10,000 foot view of Threats

Vulnerabilities 123

Compliance issues 88

Open Issues

Critical risk 35 ↑

High risk 1337 ↑

Medium risk 109 ↓

Low risk 123 ↓

Info risk 35 ↓

Protect APIs with PII data from Data Breaches

THREAT CANARY: END TO END API CAPABILITY

DISCOVER
A threat summary view of your complete API landscape.

MATURE
Red-team style vulnerability assessment and automation.

MONITOR
Monitoring of APIs. Both run-time monitoring and attack traffic.

AI/ML
AI advisors for guidance and internal LLM assisted intelligence.

BLOCK
Detect and block data breaches in progress.

REPORT
Drive exec, risk and security based report views.

TRIAGE
Vulnerability Management triage and correlation.

REMEDIATE
LLM enabled advice to support development to remediate.

Agenda

What you will learn

- **Cyberwar is inevitable**
- **Cyberwar is already here**
- **Cultural Change for the board, the CISO and Australia to survive a Cyberwar**
- **How to help Australia become more secure by 2030**

Who are we?

Audience participation time

- What is your role?
  - CIO or CTO
  - CISO
  - Manager
  - Analyst/Engineer/GRC/Consultant

Cyberwar

is inevitable

The Next Fight - The US/China War

Memo sent to Airforce

SUBJECT: February 2023 Orders in Preparation for — The Next Fight

SITUATION. I hope I am wrong. **My gut tells me we will fight in 2025.** [Chinese President Xi Jinping] secured his third term and set his war council in October 2022. Taiwan's presidential elections are in 2024 and will offer Xi a reason. United States' presidential elections are in 2024 and will offer Xi a distracted America. Xi's team, reason, and opportunity are all aligned for 2025. We spent 2022 setting the foundation for victory. We will spend 2023 in crisp operational motion building on that foundation.

General Mike Minihan

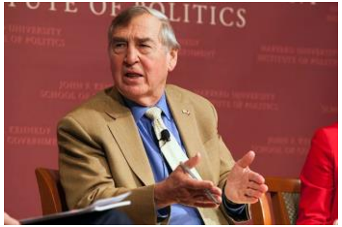
- Four-star US General
- US Air Mobility Command

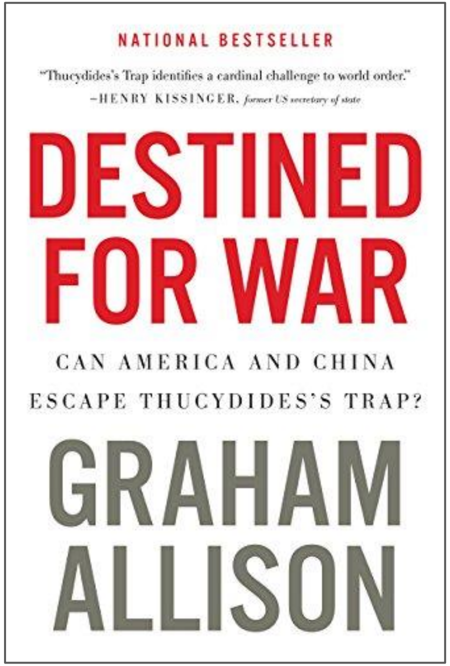
The Thucydides Trap

“When a rising power threatens to displace a ruling power, the resulting structural stress makes a violent clash the rule, not the exception.”

Graham Allison

- American Politician Scientist
- Professor at JFK Gov School at Harvard
- United States Assistant Secretary of Defense for Policy and Plans (1993–1994)





NATIONAL BESTSELLER

“Thucydides’s Trap identifies a cardinal challenge to world order.”
—HENRY KISSINGER, *former US secretary of state*

DESTINED FOR WAR

CAN AMERICA AND CHINA ESCAPE THUCYDIDES’S TRAP?

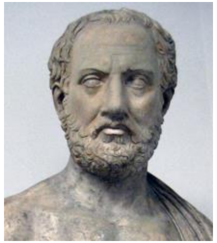
GRAHAM ALLISON

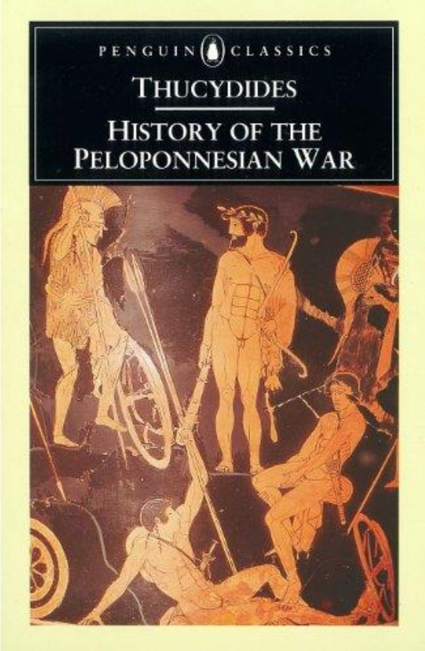
The Peloponnesian War

"It was the rise of Athens and the fear that this instilled in Sparta that made war inevitable."

Thucydides

- Athenian General
- Wrote the History of the Peloponnesian War
- Exiled after losing a battle





PENGUIN CLASSICS

THUCYDIDES

HISTORY OF THE PELOPONNESIAN WAR

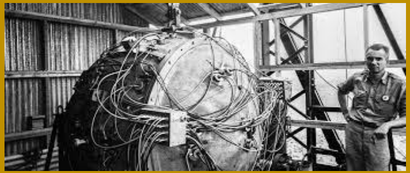
War and Technology

World War I

The Chemists' War

World War II

The Physicists' War



First Gulf War

Electronic Warfare

The Next Big War

Will begin with Cyber

The Next Big War

“The first shots fired in any war will not be bullets, but bits and bytes, disabling your military systems and civil infrastructure”

The Hon Scott Morrison

- Former Australian Prime Minister
- BSC Hons in Economic Geography
- Australia's first Pentecostal prime minister

Cyberwar

is already here

Are we on the precipice of war?

“Our Government’s view is that Australia faces the most dangerous set of strategic circumstances since the Second World War.”

The Hon Clare O’Neil MP

- Australian Minister for Home Affairs and Cyber Security
- Youngest female Mayor in Australian history
- Former McKinsey & Company consultant
- Fulbright Scholar

Are we already in an undeclared Cyberwar?

“In many ways, we may not even know when a cyber attack or indeed when a cyber campaign against Australian interests has begun,”

Rory Metcalf

- Head of the National Security College (NSC) at the Australian National University (ANU)
- Australian Former Diplomat
- Former Senior Strategic Analyst with the Office of National Assessments

Unrestricted Warfare Book

Unrestricted Warfare in 1999

“using all means, including armed force or non-armed force, military and non-military, and lethal and non-lethal means to compel the enemy to accept one's interests."

“War was confined to the ‘military sphere’, but now outcomes can be decided by, “political factors, economic factors, diplomatic factors, cultural factors, technological factors, or other nonmilitary factors.”

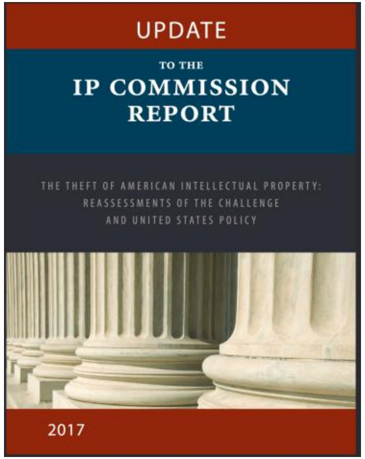
Qiao Liang (乔良) and Wang Xiangsui (王湘穗)

- Wrote Unrestricted Warfare in 1999
- Qiao Liang: retired Major General, military theorist and author.
- Wang Xiangsui: retired Senior Colonel and Professor in Beijing.

Chinese Intellectual Property Theft from the US

IP Commission Report in 2013, and updated in 2017

“We estimate that at the low end the annual cost to the U.S. economy of several categories of IP theft exceeds $225 billion, with the unknown cost of other types of IP theft almost certainly exceeding that amount and possibly being as high as $600 billion annually”



UPDATE

TO THE

IP COMMISSION REPORT

THE THEFT OF AMERICAN INTELLECTUAL PROPERTY: REASSESSMENTS OF THE CHALLENGE AND UNITED STATES POLICY

2017

Chinese Intellectual Property Theft from the US

United States Response

- 2014 Indicted five members of PLA unit 61398 in Shanghai
- Economic espionage charges

Names

- APT 1, Comment Crew, Comment Panda, GIF89a, Byzantine Candor, Group 3, Threat Group 8223

HQ in Pudong, Shanghaia

Tik-Tok

TikTok, is a “useful propaganda tool for the Chinese Communist Party.”

Lawsuit Alleges

- TikTok functioned as a “propaganda” arm of China
- ByteDance had a culture of lawlessness and stole videos from Instagram and SnapChat
- The CCP (Chinese Communist Party) had full access to all Tik-Tok data
- A secret CCP office at ByteDance where a committee monitored how “core Communist values” were being advanced.

Yintao "Roger” Yu

- Whistle-blower
- Suing ByteDance in San Francisco Court
- Head of engineering in US for ByteDance (Tik-Tok’s parent company.

Tik-Tok

“One-third of the adult population receives their news from this app, one-sixth of our children are saying they are constantly on this app, if you consider that there’s 150 million people every single day that are obviously touching this app, this provides a foreign national a platform for information operations, a platform for surveillance”

Gen. Paul M. Nakasone

- United States Army General
- Commander of U.S. Cyber Command
- Director of the National Security Agency

Chinese APT Groups

Too many Chinese APTs to list

Group	Targets	Techniques
APT25	The defense industrial base, media, financial services, and transportation sectors in the U.S. and Europe.	Spear phishing
APT27	multiple organizations headquartered around the globe, including North and South America, Europe, and the Middle East. These organizations fall into a range of different industries, including business services, high tech, government, and energy; however a notable number are in the aerospace and transport or travel industries.	Spear phishing and vulnerable web applications.
APT30	Members of the Association of Southeast Asian Nations (ASEAN)	Can cross air-gapped networks. Register their own DNS domains for malware CnC.
APT31	Multiple, including government, international financial organization, and aerospace and defense organizations, as well as high tech, construction and engineering, telecommunications, media, and insurance.	Java and Adobe Flash
APT40	maritime targets, defense, aviation, chemicals, research/education, government, and technology organizations.	Spear-phishing. Leverages compromised email addresses.
APT41	healthcare, telecoms, and the high-tech sector, ideo game industry targeting	Spear-phishing emails with attachments such as compiled HTML (.chm) files. Uses rootkits and bootkits.

Chinese APTs use Zero Days

Zero Day Exploits

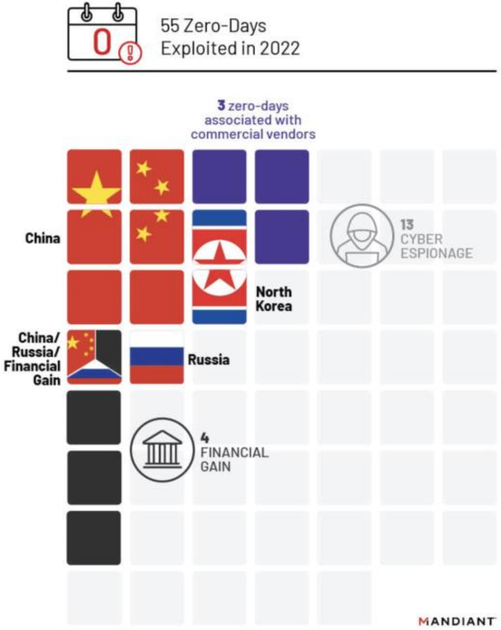
“Chinese state-sponsored cyber espionage groups exploited more zero-days than other cyber espionage actors in 2022, which is consistent with previous years.”- Mandiant (Google) Threat Intelligence

Focus on Enterprise Networking & Security Devices

- Fortinet's FortiOS SSL-VPN (CVE-2022-42475 and CVE-2022-41328)
- FortiManager FortiOS (CVE-2022-41328)

Spear Phishing with Microsoft Word Attachments

- Word Document exploits using Microsoft Diagnostics Tool (MDST) CVE-2022-30190
- CVE-2022-30190 also used to exploit targets in Belarus and Russia in May 2022 during the Ukraine war.

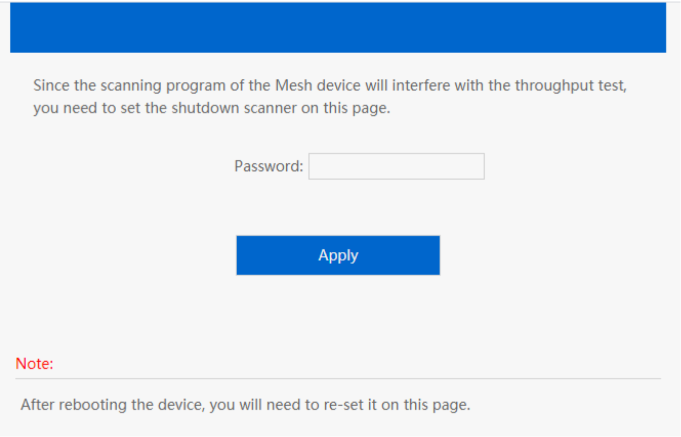


Chinese Backdoors in Products

Backdoored?

- Wavlink brand routers sold on Amazon, eBay, MWave, Dick Smith, and Kogan
- Jetstream brand exclusive to WalMart in US (Same)
- Both Linked to Winstars Technology Ltd in Shenzhen

Login form



Since the scanning program of the Mesh device will interfere with the throughput test, you need to set the shutdown scanner on this page.

Password:

Note:

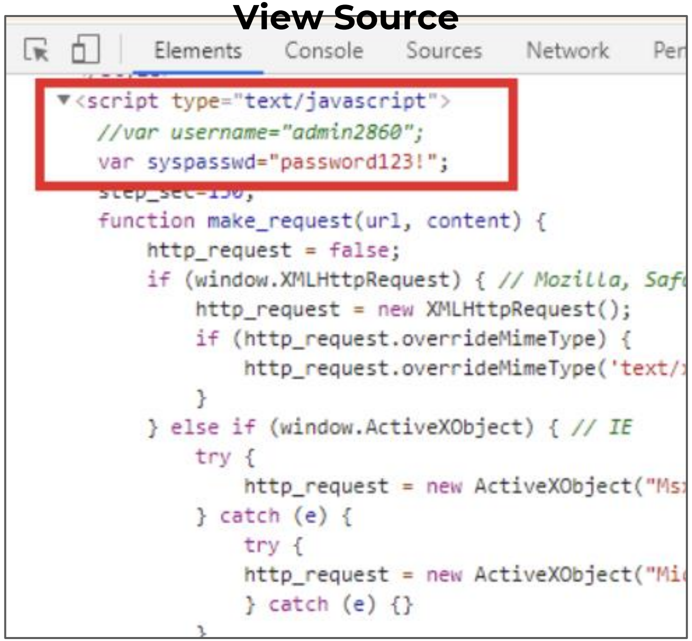
After rebooting the device, you will need to re-set it on this page.

Chinese Backdoors in Products

Backdoored?

- **Multiple Vulnerabilities in Wavlink Router leads to Unauthenticated RCE** – CVE-2020-10971 and CVE-2020-10972
- Exploited by Mirai botnet since 2020

View Source



```
▼<script type="text/javascript">
  //var username="admin2860";
  var syspasswd="password123!";
  step_sec=150;
  function make_request(url, content) {
      http_request = false;
      if (window.XMLHttpRequest) { // Mozilla, Safa
          http_request = new XMLHttpRequest();
          if (http_request.overrideMimeType) {
              http_request.overrideMimeType('text/x
          }
      } else if (window.ActiveXObject) { // IE
          try {
              http_request = new ActiveXObject("Msx
          } catch (e) {
              try {
              http_request = new ActiveXObject("Mic
              } catch (e) {}
          }
```

Microsoft O365 Enterprise Email Shopping Spree

Major Email Compromise in April 2023

- Email stolen from up to 25 organisations including the US State Department
- APT Group: STORM-0558
- Wiz analysis indicates the compromise could go far beyond email

Highly Complex Attack Chain

- Microsoft engineer account compromised with Malware to gain access to crash dumps
- Crash dumps contained an Azure Signing Key (Moved from Prod to Debugging Env)
- Secrets detection for crash dumps failed
- Generated new Microsoft account tokens
- Exploited a bug in an API that validated tokens (Consumer keys accepted as Enterprise keys)

Chinese Cyberwar

Economic Warfare

- Theft of Intellectual Property

Beijing in your Supply Chain

- Backdoors and Bugdoors

Sophisticated

- Wide range of sophistication among APT groups
- Attacking Clouds like Microsoft

Spear phishing

- Phishing “just works”
- Using zero-days

Unrestricted Warfare

- Not just cyberwar - Mixing in all kinds of non-military war including economic and cultural warfare

What does Russian Cyberwar look like?

The NotPetya Cyberweapon

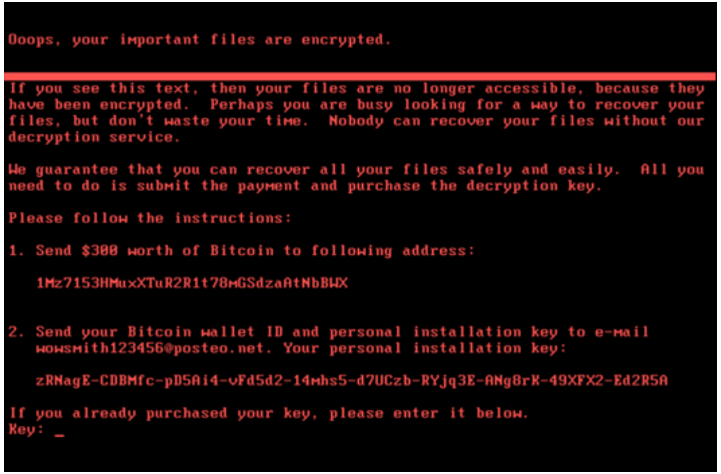
- Repurposed Petya, a ransomware software
- Demands payment in BTC and does not unlock

The Attack

- 27 June 2017 massive infection across Ukraine
- Attack originated from an update of a Ukrainian tax accounting package called MeDoc used by 90% of Ukrainian companies

Attack Vector

- Used the EternalBlue exploit (NSA)
- Encrypted files



```
Ooops, your important files are encrypted.

If you see this text, then your files are no longer accessible, because they
have been encrypted.  Perhaps you are busy looking for a way to recover your
files, but don't waste your time.  Nobody can recover your files without our
decryption service.

We guarantee that you can recover all your files safely and easily.  All you
need to do is submit the payment and purchase the decryption key.

Please follow the instructions:

1. Send $300 worth of Bitcoin to following address:

   1Mz7153HMuxXTuR2R1t78mGSdzaAtNbBWX


2. Send your Bitcoin wallet ID and personal installation key to e-mail
   wowsmith123456@posteo.net. Your personal installation key:

   zRNagE-CDBMfc-pD5Ai4-vFd5d2-14mhs5-d7UCzb-RYjq3E-ANg8rK-49XFX2-Ed2R5A

If you already purchased your key, please enter it below.
Key: _
```

Attribution

- Sandworm is an APT
- Military Unit 74455, a cyberwarfare unit of the GRU, Russia's military intelligence service

What does Russian Cyberwar look like?

The Viasat Hack

- Targeted Viasat KA-SAT modems across the Ukraine
- Wiped residential satellite modems

Staging

- The Viasat company in the United States was targeted
- Attackers used a poorly configured virtual private network appliance to gain access to the trusted management part of the KA-SAT network

The Cyber Attack

- Viasat modems were bricked on the day Russia invaded Ukraine
- A firmware update was sent out to thousands of Viasat modems across the world.

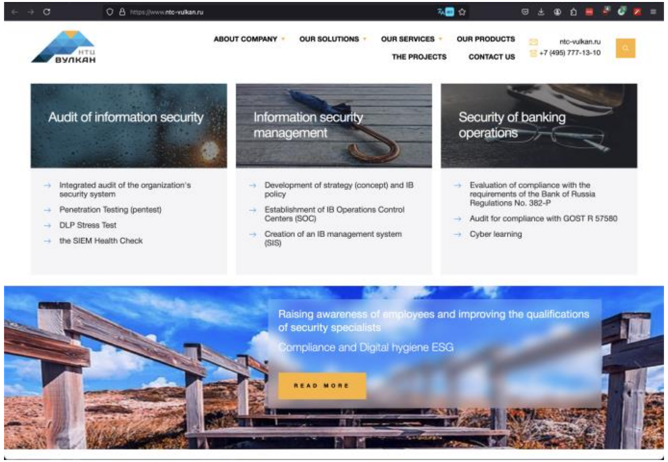
Russian APT Groups

There are more

Group	Operator	Targets	Techniques
APT28, Fancy Bear, Pawn Storm, Sofacy Group, Sednit, STRONTIUM, Tsar Team, Threat Group-4127, Grizzly Steppe (+APT29)	GRU Unit 26165	Norwegian Parliament, German Council on Foreign Relations, International Republican Institute, International Olympic Committee, German and French elections, Dutch ministries, US Democratic National Committee, Whitehouse, NATO, French TV5Monde, Bank of America, United Bank for Africa, UAE Bank, Media and journalists.	Windows Zero-days, Java Zero-days, Spear-phishing, and malware
APT29, Cozy Bear, CozyCar, CozyDuke, Dark Halo, The Dukes, Grizzly Steppe (+APT28), NOBELIUM, Office Monkeys, StellarParticle, UNC2452, YTTRIUM	Probably the Russian Federal Security Service (FSB) or SVR	The US Pentagon, US think tanks and NGOs, Norwegian government, Dutch ministries, SolarWinds, Republican National Committee, Microsoft customers.	Spear-phishing, MagicWeb attack through Active Directory Federated Services, and malware
Beserk Bear, Crouching Yeti, Dragonfly Dragonfly 2.0, DYMALLOY, Energetic Bear, Havex, IRON LIBERTY, Koala, TeamSpy	FSB + civilian + criminal hackers	Water and energy utilities. Airports.	Malware
Sandworm, Voodoo Bear, Iron Viking, Telebots	GRU Unit 74455	Ukraine, Electrical Utilities in the Ukraine, 2018 Winter Olympics, Parliament of Georgia, Organization for the Prohibition of Chemical Weapons in the Hague.	Zero-days, spearphishing, malware, router botnets, fake ransomware (NotPetya), BlackEnergy, Industroyer

Russian Vulkan Leak

- Moscow based Russian NTC Vulkan
- Cyber and Defence Contractor
- Leak of 5000+ documents



https://www.ntc-vulkan.ru

НТЦ ВУЛКАН

ABOUT COMPANY | OUR SOLUTIONS | OUR SERVICES | OUR PRODUCTS | THE PROJECTS | CONTACT US

ntc-vulkan.ru

+7 (495) 777-13-10

Audit of information security

- Integrated audit of the organization's security system
- Penetration Testing (pentest)
- DLP Stress Test
- the SIEM Health Check

Information security management

- Development of strategy (concept) and IB policy
- Establishment of IB Operations Control Centers (SOC)
- Creation of an IB management system (SIS)

Security of banking operations

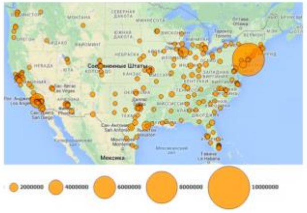
- Evaluation of compliance with the requirements of the Bank of Russia Regulations No. 382-P
- Audit for compliance with GOST R 57580
- Cyber learning

Raising awareness of employees and improving the qualifications of security specialists

Compliance and Digital hygiene ESG

READ MORE

Leak shows Cyber Targeting of Civilian Infrastructure



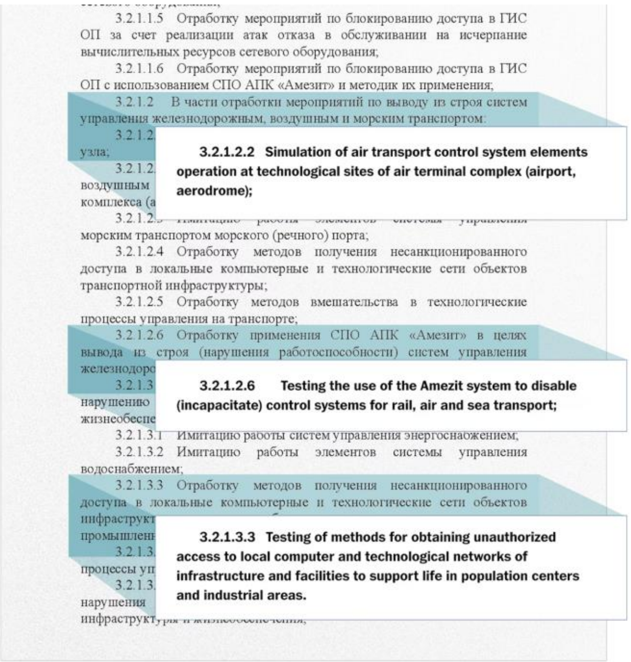
Linked to

- GRU / Sandworm / Unit 74455
- Cozy Bear

Russian Vulkan Leak Projects

Leaked documentation for offensive cyber capabilities

Scan-V	● Scans of the internet ● Targets civilian infrastructure ● Using Nmap & Nessus
Amezit-V	● Discovery & Mapping of Critical Infrastructure ● Railways & Power Plants ● USB Plug-in with Physical access
Krystal-2V	● Educational & Training ● Offensive & Defensive Scenarios ● Disable Rail, Air, Sea Transport



сетевого оборудования;

3.2.1.1.5 Отработку мероприятий по блокированию доступа в ГИС ОП за счет реализации атак отказа в обслуживании на исчерпание вычислительных ресурсов сетевого оборудования;

3.2.1.1.6 Отработку мероприятий по блокированию доступа в ГИС ОП с использованием СПО АПК «Амезит» и методик их применения;

3.2.1.2 В части отработки мероприятий по выводу из строя систем управления железнодорожным, воздушным и морским транспортом:

3.2.1.2.

узла;

3.2.1.2.

воздушным

комплекса (а

3.2.1.2.3 Имитацию работы элементов системы управления морским транспортом морского (речного) порта;

3.2.1.2.4 Отработку методов получения несанкционированного доступа в локальные компьютерные и технологические сети объектов транспортной инфраструктуры;

3.2.1.2.5 Отработку методов вмешательства в технологические процессы управления на транспорте;

3.2.1.2.6 Отработку применения СПО АПК «Амезит» в целях вывода из строя (нарушения работоспособности) систем управления железнодоро

3.2.1.3

нарушению

жизнеобеспе

3.2.1.3.1 Имитацию работы систем управления энергоснабжением;

3.2.1.3.2 Имитацию работы элементов системы управления водоснабжением;

3.2.1.3.3 Отработку методов получения несанкционированного доступа в локальные компьютерные и технологические сети объектов инфраструкт

промышлен

3.2.1.3.

процессы уп

3.2.1.3.

нарушения

инфраструктуры и жизнеобеспечения;

3.2.1.2.2 Simulation of air transport control system elements operation at technological sites of air terminal complex (airport, aerodrome);

3.2.1.2.6 Testing the use of the Amezit system to disable (incapacitate) control systems for rail, air and sea transport;

3.2.1.3.3 Testing of methods for obtaining unauthorized access to local computer and technological networks of infrastructure and facilities to support life in population centers and industrial areas.

Russian Cyberwar

No Attribution

- Pretending to be other groups
- Masquerading as Ransomware
- Knocking out power in the Ukraine during winter

Psychological

- Causing blackouts in Ukraine in winter
- Data breaches to demoralise

Data Wipers

- Denial of service

Data Breaches

- Sharing personal data from databases

Collateral Damage

- Non-combatants being attacked

The Attribution Problem

“For more than two decades, cyber defenders, intelligence analysts, and policymakers have struggled to determine the source of the most damaging attacks. This attribution problem will only become more critical as we move into a new era of cyber conflict with even more attacks ignored, encouraged, supported, or conducted by national governments”

Jason Healey

- Senior Research Scholar at Columbia University
- Senior Fellow of the Cyber Statecraft Initiative of the Atlantic Council
- Ex-Goldman Sachs, Director for Cyber Infrastructure Protection at the White House, US Air-force, and more.
- Pioneer of Threat Intelligence
- Author

“who is to blame?” can be more important than “who did it?”

Continuous Attacks on Australia

Who’s hacking us?

Date	Victim	Industry	Attribution	Data Breach
May 2024	XM Group	Investment	Wht forum user	More than 400k customers. Full name, gender, email, date of birth, phone number, street name, city, AUD, assets, postcode, and website.
May 2024	Sumo	Energy and ISP	OriginalCrazyOldFart forum user	Insecure Amazon S3 Buckets Names, addresses, dates of birth, phone numbers, credit scores, as well as either passport, Medicare, or driver’s licence details.
May 2024	Dell	Computers	Menelik forum user	seven million rows of individual purchases, and 11 million rows of "consumer segment companies," while the rest are enterprise-grade customers, Dell partners, and schools United States, China, India, Australia, and Canada.
May 2024	ZircoDATA	Secure Document Storage and Destruction	Black Basta Ransomware Gang	395 GB of data. Example: Monash Health with family violence and sexual assault documents from 1970-1993
May 2024	Clubs NSW	Bowling, League, and RSL Clubs	Phillipines software devs (unpaid and disgruntled)	More than 1m records. Personal IDs like Drivers Licenses, phone numbers, and slot machine usage.

Continuous Attacks on Australia

Too many to list

Date	Victim	Industry	Attribution	Data Breach
February 2024	Victorian Court System	Government	Qilin ransomware (Russian)	Ransomware attack. 7 weeks of Supreme, County, Coroners, Appeals, Children’s, etc.
November 2023	Alfred Health	Health	?	Patient data, HIV status, etc
June 2023	ACT Government	Gov	?	Email
May 2023	Fire Rescue Victoria	Fire	?	Identification and contact information, but also medical records, passport and driver's license details, Medicare numbers, Centrelink numbers and healthcare identifiers.
May 2023	HWL Ebsworth	Law	AlphV ransomware (Russian)	1.45 terabytes of data. Wide range of corporate and gov clients.
March 2023	Latitude	Financial	?	14m customers. Drivers license numbers, passports, etc.
December 2022	Medibank	Insurance	REvil ransomware (Russian)	9.7m people’s records
Sept 2022	Optus	Telco	?	9.8m customers.

Cultural Change

For the CISO

Security is a process

Process vs product:

- *Is not a product*
- *Is not a team within Cyber*
- *Is a process*

"Security is a process, not a product. Products provide some protection, but the only way to effectively do business in an insecure world is to put processes in place that recognize the inherent insecurity in the products. The trick is to reduce your risk of exposure regardless of the products or patches."

Bruce Schneier

- American cryptographer, security pro, privacy specialist, and writer.
- Lecturer at Harvard Kennedy School
- Influential security blogger.
- Serial author.

Processs: Henry Ford’s Assembly Line

Henry Ford invented the assembly line

- Automation at every step
- Increasing release speed
- Improving release quality

Cultural change

- Different teams working together
- Unskilled labour can build cars.

Lift scaling limits on labour

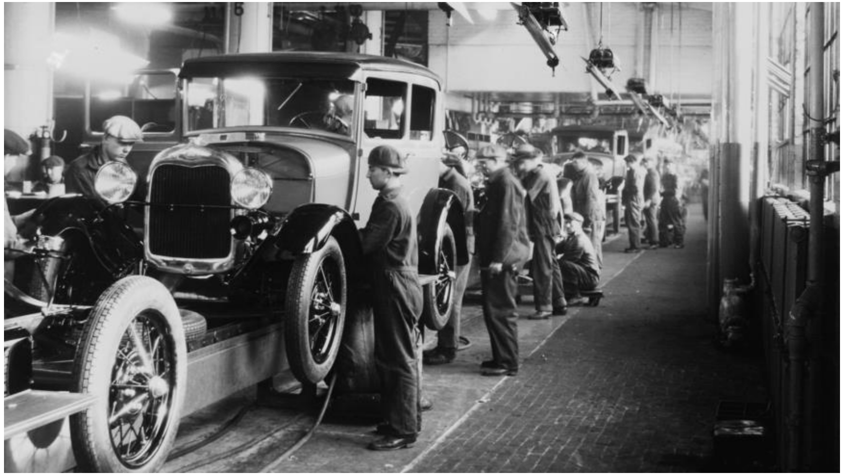
- No longer limited by skilled engineers.

By 1912 Ford’s key concepts

- Repeatable processes
- Standardized inputs / output

Relies on

- Industrial revolution



Ford Model T Assembly Line at the Highland Park Plant, 1915

100 years later: DevOps

Continuous Integration / Continuous Deployment

- Automation at every step
- Increasing release speed
- Improving release quality

Cultural Change

- Different teams working together
- Agile methodology

Lift scaling limits on labour

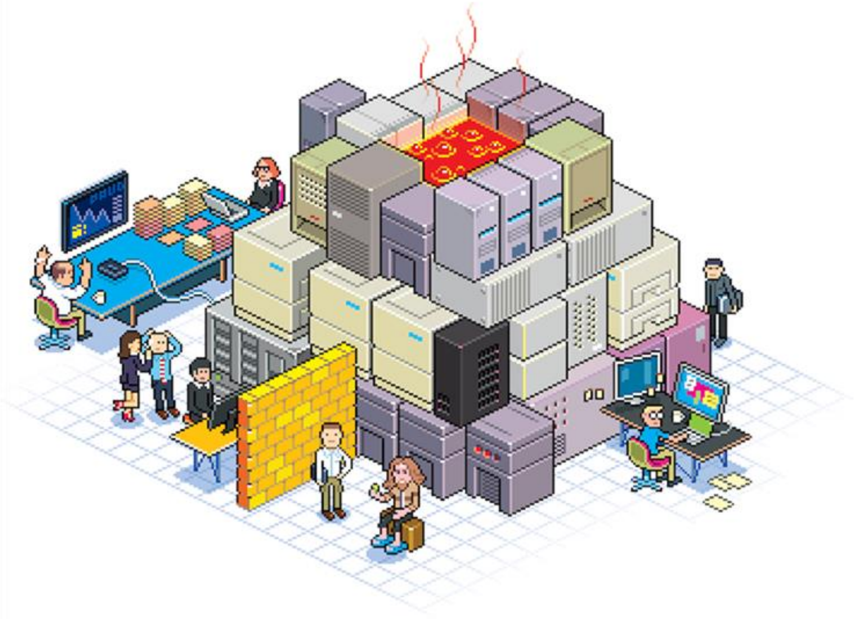
- No longer limited by skilled engineers

DevOps Key Concepts

- Repeatable processes
- Standardized inputs / output

Relies on

- Open-source software components (interchangeable parts)



The Phoenix Project
A Novel about IT, DevOps, and Helping Your Business Win

DevSecOps is Cultural Change

Continuous Security

- Automation of security at every step
- Increasing release speed
- Improving release quality

Cultural Change

- Different teams working together
- Shift security left and everyone is responsible

Lift scaling limits on labour

- No longer limited by skilled red and blue teams.

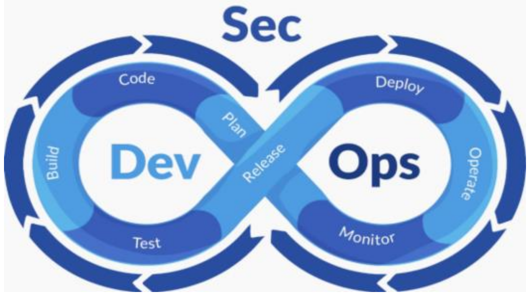
DevSecOps Key Concepts

- Repeatable processes
- Standardized inputs / output

Relies on

- DevOps
- DAST, SAST, SCA, and other tools

The DevSecOps Lifecycle



"DevSecOps is using automation to take responsibility for vulnerabilities in your own development."

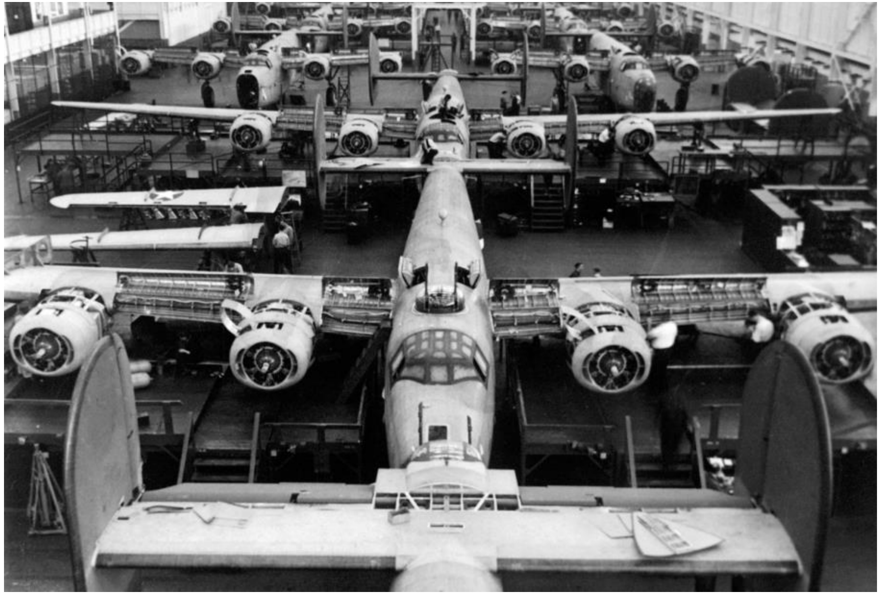
Ford’s Assembly Line Helped Win WWII

The B-24 Liberator bomber

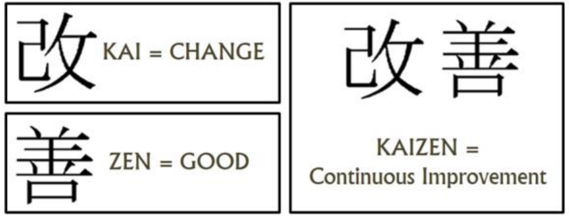
- The most mass-produced US military aircraft of all time.
- Built by the Ford Motor company

By 1945 Ford was building B-24 Liberators at a rate of one per hour.

“The production miracle of the war”,
The Wall Street Journal



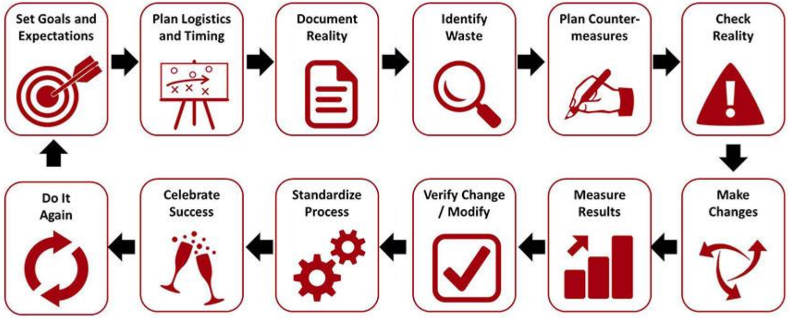
Management Philosophy of Kaizen


改 KAI = CHANGE

善 ZEN = GOOD

改善

KAIZEN = Continuous Improvement


Set Goals and Expectations

Plan Logistics and Timing

Document Reality

Identify Waste

Plan Counter-measures

Check Reality

Make Changes

Measure Results

Verify Change / Modify

Standardize Process

Celebrate Success

Do It Again

Masaaki Imai

- Japanese Organizational Theory and Management Consultant
- Father of Continuous Improvement
- Published “Kaizen, the Key to Japan’s Competitive Success”:

Reporting to the Board

Dashboards

- Avoid bespoke dashboards and reporting. Take screenshots of dashboards in your existing tools then add commentary.
- Be careful with frameworks like NIST CSF because they are subjective.
- Don't be afraid to say maturity is low and you are working towards moderate security

"What gets measured gets managed – even when it's pointless to measure and manage it, and even if it harms the purpose of the organisation to do so."

This quote is often misattributed to management guru, Peter Drucker

V.F. Ridgway

- Published in Administrative Science Quarterly in 1956

Stop saying “No”

Cyber often becomes “No as a Service”

- There is a cultural battle for Cyber to win over the hearts and minds of Devs and Ops teams.
- Enable IT securely rather than being a tax on productivity.
- Look for creative ways to say yes while remaining secure.
- Shadow IT is a result of saying no too often.
- The “Noers” are holding everyone back.

Cultural Change

For the Board
& Senior Leadership

Who should the CISO report to?

In many organizations the CISO reports to the CIO, CTO or CRO.

- Inherent conflicts of interest
- CIO/CTO decisions may lead to insecurity

In more mature organizations

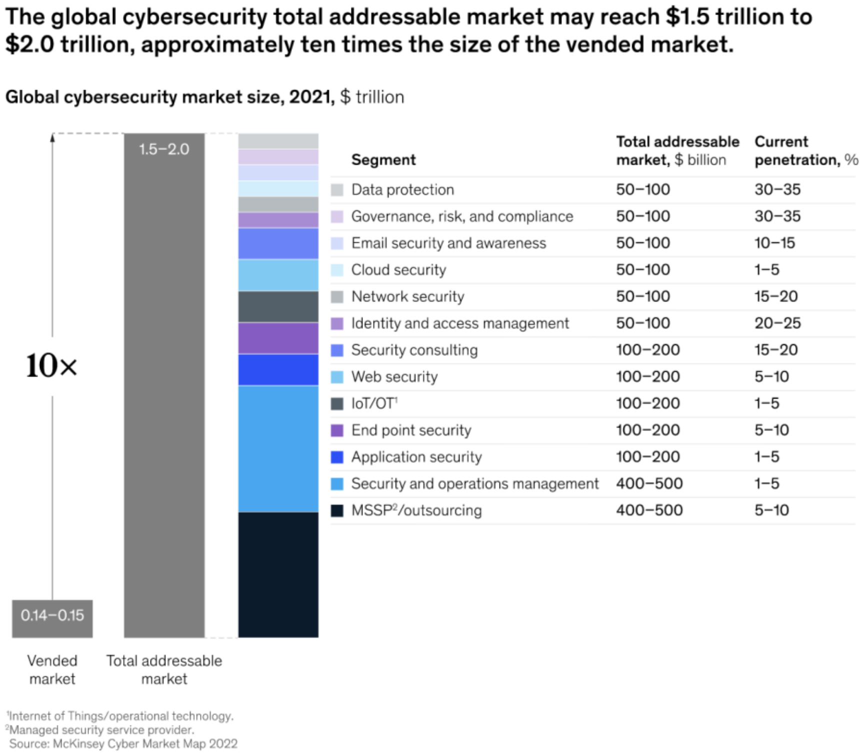
- The CISO reports to the CEO or a board member

> *"One simple way to improve cybersecurity: Promote CISOs to report into CEOs."*

Jeff Pollard

- VP & Principal Analyst at Forrester
- Directs research on CISO Strategy
- Global Architect at Verizon
- Principal Architect at Mandiant

Cultural change requires budget change



The global cybersecurity total addressable market may reach $1.5 trillion to $2.0 trillion, approximately ten times the size of the vended market.

Global cybersecurity market size, 2021, $ trillion

Segment	Total addressable market, $ billion	Current penetration, %
■ Data protection	50–100	30–35
■ Governance, risk, and compliance	50–100	30–35
■ Email security and awareness	50–100	10–15
■ Cloud security	50–100	1–5
■ Network security	50–100	15–20
■ Identity and access management	50–100	20–25
■ Security consulting	100–200	15–20
■ Web security	100–200	5–10
■ IoT/OT[1]	100–200	1–5
■ End point security	100–200	5–10
■ Application security	100–200	1–5
■ Security and operations management	400–500	1–5
■ MSSP[2]/outsourcing	400–500	5–10

[1] Internet of Things/operational technology.
[2] Managed security service provider.
Source: McKinsey Cyber Market Map 2022

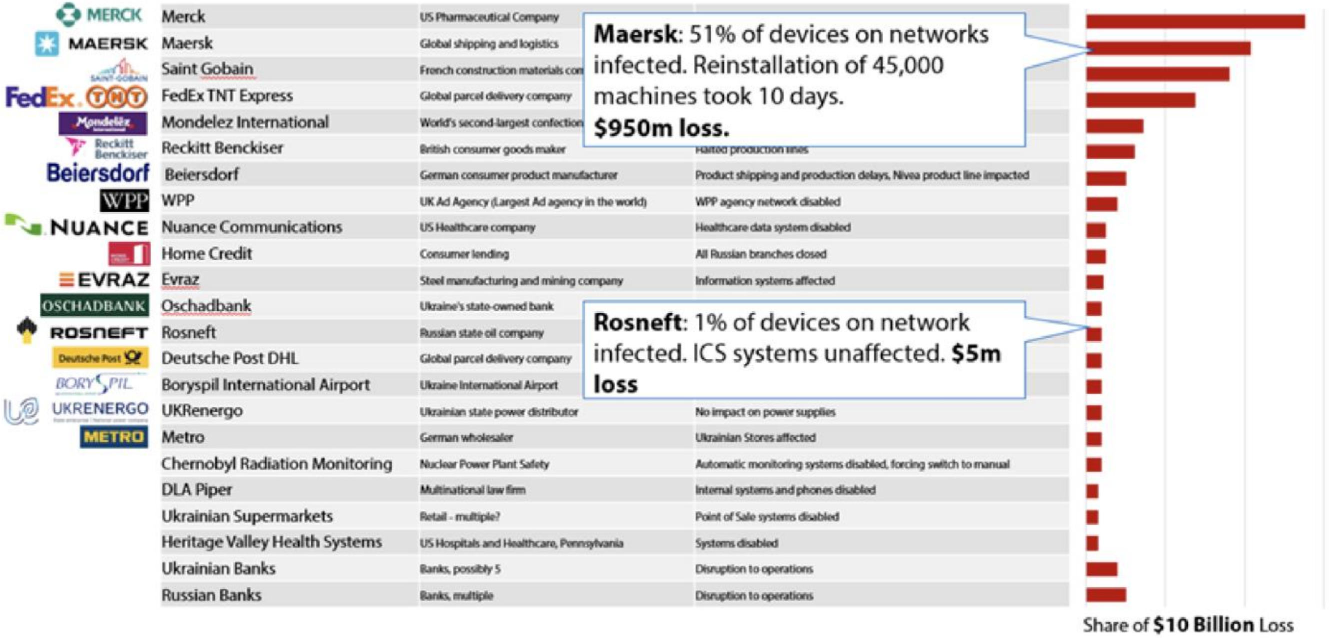
> *"The under-penetration of cybersecurity products and services […] suggests that the budgets of many if not most chief information security officers (CISOs) are underfunded"*

McKinsey & Company

Bharath Aiyer, Jeffrey Caso, Peter Russell, and Marc Sorel **McKinsey & Company**

Forget about Cyber Insurance

Figure 10: Companies Impacted by NotPetya Ransomware Event in 2017 (Source: CCRS Analysis).



Merck	US Pharmaceutical Company	
Maersk	Global shipping and logistics	
Saint Gobain	French construction materials com	
FedEx TNT Express	Global parcel delivery company	
Mondelez International	World's second-largest confection	
Reckitt Benckiser	British consumer goods maker	Halted production lines
Beiersdorf	German consumer product manufacturer	Product shipping and production delays, Nivea product line impacted
WPP	UK Ad Agency (Largest Ad agency in the world)	WPP agency network disabled
Nuance Communications	US Healthcare company	Healthcare data system disabled
Home Credit	Consumer lending	All Russian branches closed
Evraz	Steel manufacturing and mining company	Information systems affected
Oschadbank	Ukraine's state-owned bank	
Rosneft	Russian state oil company	
Deutsche Post DHL	Global parcel delivery company	
Boryspil International Airport	Ukraine International Airport	
UKRenergo	Ukrainian state power distributor	No impact on power supplies
Metro	German wholesaler	Ukrainian Stores affected
Chernobyl Radiation Monitoring	Nuclear Power Plant Safety	Automatic monitoring systems disabled, forcing switch to manual
DLA Piper	Multinational law firm	Internal systems and phones disabled
Ukrainian Supermarkets	Retail - multiple?	Point of Sale systems disabled
Heritage Valley Health Systems	US Hospitals and Healthcare, Pennsylvania	Systems disabled
Ukrainian Banks	Banks, possibly 5	Disruption to operations
Russian Banks	Banks, multiple	Disruption to operations

Maersk: 51% of devices on networks infected. Reinstallation of 45,000 machines took 10 days. **$950m loss.**

Rosneft: 1% of devices on network infected. ICS systems unaffected. **$5m** **loss**

Cambridge Centre for Risk Studies

Maersk's insurers failed to argue it was exempt because it was an act of war.

In 2023 insurers were ordered to pay out $2b AUD or $1.4b USD in damages

Forget about Cyber Insurance

Lloyd’s

- World’s leading marketplace for insurance and reinsurance
- Stopped covering nation state-attacks in October, 2023

Lloyd’s and Cambridge Centre for Risk Studies Published

- 3.3% or 1-in-30-year probability of a hypothetical scenario
- They *estimate losses of $3.5 trillion* from the global economy as a result of a major cyberattack targeting payment systems

“Cyber insurance is a growing market, estimated at just over $9bn in Gross Written Premiums last year, and forecast to hit between $13bn and $25bn by 2025. However this still represents a small portion of the potential economic losses that businesses and society face.”

You will have to defend yourself

The Age of Sail vs The Age of Cyber

- It is an age of pirates and privateers fighting for themselves and for nation-states.
- It is an age of letters of marque. Where some pirates were legally permitted to plunder Spanish merchant ships.
- It is an age of false flag attacks. It was common for pirates to fly whatever flag suited them.
- You wouldn't know if their spies read your letters either.
- You are profiting from the far side of the world with new naval technology. Beyond your government's reach.

- It is an age of ransomware groups and financial crime.
- Some crime groups are nation-state backed and others are state-tolerated as long as they ransomware or hack foreigners.
- It is an age of misattribution attacks and sophisticated deep-fakes.
- You won't always know when cyber attacked.
- You are profiting from being on the Internet that's open to the rest of the world. Beyond your government's reach.

Pirates, APTs and Ransomware Groups

	State-backed	State-tolerated		
Pirates	Privateers			
Russian APTs and Ransomware Groups		Russian cyber gangs are tolerated		

The Age of Sail vs The Age of Cyber

- It is an age of pirates and privateers fighting for themselves and for nation-states.
- It is an age of letters of marque. Where some pirates were legally permitted to plunder Spanish merchant ships.
- It is an age of false flag attacks. It was common for pirates to fly whatever flag suited them.
- You wouldn't know if their spies read your letters either.

- It is an age of ransomware groups and financial crime.
- Some crime groups are nation-state backed and others are state-tolerated as long as they ransomware or hack foreigners.
- It is an age of misattribution attacks and sophisticated deep-fakes.
- You won't always know when cyber attacked.
- You are profiting from being on the Internet that's open to the rest of the world. Beyond your government's reach.

Cultural Change

For Australia

Taking down cameras was a cultural change

Chinese made surveillance cameras

- HikVision & Dahua

HIKVISION alhua TECHNOLOGY

Popular Cameras

- Good quality for the price

Cultural Change

- Removed from Australian sensitive buildings in 2023

“That [risk has] obviously been there, I might say, for some time and predates us coming into office”

Hon Richard Marles MP

- Australian Defence Minister
- Former Deputy Prime Minister
- Lawyer

HIKVISION Insecure, Backdoored, and Popular

Supply Chain Risk

Beijing in your Supplychain →

PRC’s 2017 National Intelligence Law compels any Chinese subject to spy on behalf of the state.

Australia does this too.

Backdoors

Firmware backdoor →

HikVision Firmware 2014 – 2016 Backdoor

Access without the password using the backdoor by adding auth=YWRtaW46MTEK to the URL.

`http://camera.ip/onvif-http/snapshot?auth=YWRtaW46MTEK`

Security

Published Vulnerabilities →

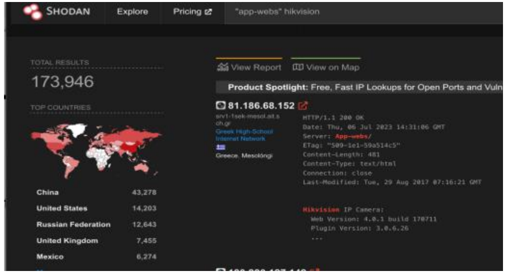
Published Vulns

CVE-2023-28808, CVE-2022-28173, CVE-2022-28172, CVE-2022-28171, CVE-2021-36260, CVE-2020-7057

Popular

173,945 found with Shodan

Directly exposed to the Internet →



TOTAL RESULTS

173,946

TOP COUNTRIES

China	43,278
United States	14,203
Russian Federation	12,643
United Kingdom	7,455
Mexico	6,274

Product Spotlight: Free, Fast IP Lookups for Open Ports and Vuln

81.186.68.152

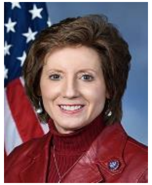
srv1-1sek-mesol.ait.s
ch.gr
Greek High-School Internet Network
Greece, Mesolóngi

```
HTTP/1.1 200 OK
Date: Thu, 06 Jul 2023 14:31:06 GMT
Server: App-webs/
ETag: "509-1e1-59a514c5"
Content-Length: 481
Content-Type: text/html
Connection: close
Last-Modified: Tue, 29 Aug 2017 07:16:21 GMT


Hikvision IP Camera:
  Web Version: 4.0.1 build 170711
  Plugin Version: 3.0.6.26
  ...
```

Chinese Military-Industrial Complex Sanctions Update

Chinese-made drones, surveillance, and security systems



“We must face the reality that the Chinese-government is using every avenue at its disposal to target the United States, including expanding the role of Chinese companies in the U.S. domestic communications and public safety sectors. Video surveillance and security equipment sold by Chinese companies exposes the U.S. government to significant vulnerabilities”

Rep. Vicky Jo Hartzler

- American Politician
- US Missouri State Representative
- Graduated Summa cum laude in Education from Missouri University

Date	Action
2019	US President Trump signs 2019 National Defense Authorization Act (NDAA). Includes an amendment from Rep. Vicky Hartzler banning defense from buying HikVision, Dahau, and Huawei.
November 2020	Trump US Presidential Executive Order 13959 bans investment in HikVision and Dahau
January 2021	Executive Order goes into effect
June 2021	The United States OFAC (Office of Foreign Assets Control) Sanctions Update CMIC-EO13959

O F A C
Office of Foreign Assets Control

Timeline for Australia taking the cameras down

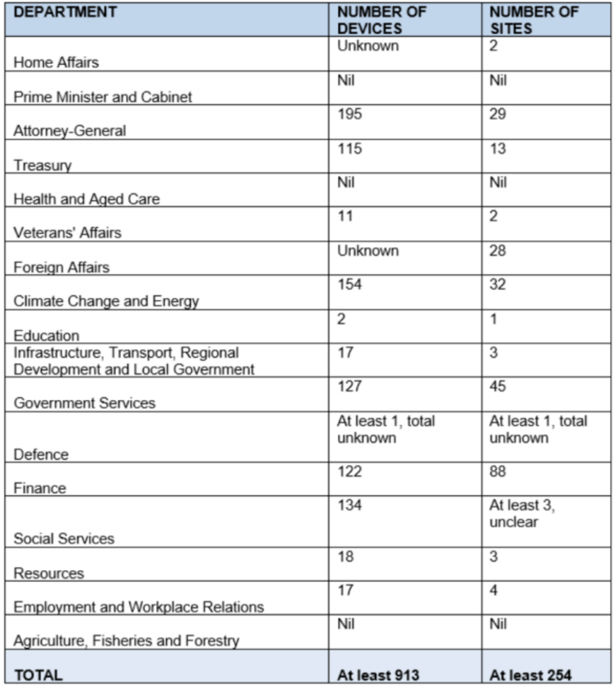
2022

Liberal Party, James Paterson asks how many Hikvision cameras Australia government has and initiates audit

"I used a software tool called Shodan, which can help identify any Internet connected devices and that show that there are at least 36,000 Hikvision devices that are Internet connected and at least 10,000 Dahua cameras that Internet connected [in Australia]."

Senator James Paterson

- Liberal Senator for Victoria
- Shadow Minister for Home Affairs and Cyber Security
- Chairs the Senate Select Committee on Foreign Interference Through Social Media
- Youngest Liberal Senator ever



DEPARTMENT	NUMBER OF DEVICES	NUMBER OF SITES
Home Affairs	Unknown	2
Prime Minister and Cabinet	Nil	Nil
Attorney-General	195	29
Treasury	115	13
Health and Aged Care	Nil	Nil
Veterans' Affairs	11	2
Foreign Affairs	Unknown	28
Climate Change and Energy	154	32
Education	2	1
Infrastructure, Transport, Regional Development and Local Government	17	3
Government Services	127	45
Defence	At least 1, total unknown	At least 1, total unknown
Finance	122	88
Social Services	134	At least 3, unclear
Resources	18	3
Employment and Workplace Relations	17	4
Agriculture, Fisheries and Forestry	Nil	Nil
TOTAL	**At least 913**	**At least 254**

Timeline for Australia taking the cameras down

2012

China Daily discusses risk of foreign surveillance equipment.

2017

Hikvision backdoor discovered. Affects 2014-2016 models.

2019

US Defence ban HikVision, Dahau and Hueawei.

2020

US Trump Presidential Executive Order 13959 prohibits investing in the cameras

2021

EU Parliament bans HikVision use in parliament.

US OFAC Sanctions Update CMIC-EO13959

2022

Liberal Party, James Paterson asks how many cameras we have and initiates audit

2022

UK and US announce banning the cameras from gov buildings

2023

Australia defence announces they took the cameras down

Cultural Change

Australian government knew the cameras were insecure and backdoored but used them anyway because they were cheap until 2023

Strategic Change

For Australia

The Cyber Security Strategy 2023-2030

Australian Government

2023–2030 Australian Cyber Security Strategy

Incidents

- A single place to report incidents – cyber.gov.au (REDSPICE initiative)
- More gov support for victims
- An Industry code of practice for incident response provider is coming...

Ransomware Attacks

- No-fault, no-liability ransomware reporting
- Anonymised ransomware reporting & intel sharing
- Australia will Chair the International Counter Ransomware Taskforce
- Crackdown on cryptocurrencies too ...

Sharing Threat Intelligence

- Executive Cyber Council is gov + industry leaders - sharing more intel with enterprises
- Threat Sharing Acceleration Fund (Health sector first)

Blocking threats

- Real time blocking at the ISP & Telco level

Voluntary Labelling

- Mandatory cyber standards for IoT
- Voluntary labelling for consumer-grade devices (with US, Singapore and UK)
- Voluntary code of practice for apps in app stores

Small & medium businesses

- 1300 CYBER
- Cyber health-check program
- Small Business Cyber Security Resilience Service

Data breaches

- Stop enterprises hoarding PII with Digital IDs (National Strategy for Identity Resilience)
- Data retention will change
- Data brokering will be reviewed

Investment

Skills shortage

- Build a cyber skills pipeline
- “Professionalise” the workforce
- TAFE Cyber Courses in the Essential 8

Cyber start ups

- Cyber Security Challenge program
- Business Research and Innovation Initiative
- Comes out of $15 billion National Reconstruction Fund (NRF) and $392.4 million Industry Growth program

Investment

- More $ for ASD and AFP.
- Project 🔥 REDSPICE 🔥 for Offensive Security R&D has $9.9b over 10 years

More critical designated Systems of National Significance

- Security of Critical Infrastructure Act 2018 (SOCI) Act
- Energy, Space technology, Food and grocery, Water and sewerage, High education and research, Financial services and markets, Health care and medical, Transport, Defence industry, Data storage or processing, and Communications

Australian Government

2023–2030
Australian Cyber
Security Strategy

Response to Malicious Cyber Actors

Australian Government

2023–2030 Australian Cyber Security Strategy

Strategy Document says Australia will:

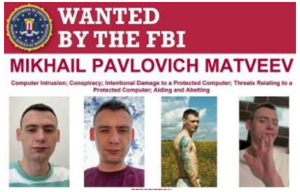
- “Deploy all arms of statecraft to deter and respond to malicious cyber actors”
- “Uphold existing international law and the agreed voluntary norms of responsible state behaviour in cyberspace”

Australia already responds:

AFP and Australian Signals Directorate (ASD) Operation Aquila started in November 2022.

Mission is to investigate, target and disrupt cybercriminal syndicates, with a priority on ransomware threat groups.

Lockbit Ransomware



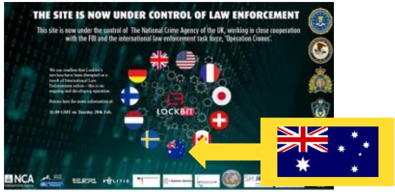
WANTED BY THE FBI

MIKHAIL PAVLOVICH MATVEEV

Computer Intrusion; Conspiracy; Intentional Damage to a Protected Computer; Threats Relating to a Protected Computer; Aiding and Abetting

Russian wanted

Arrests in Ukraine & Poland



THE SITE IS NOW UNDER CONTROL OF LAW ENFORCEMENT

This site is now under the control of The National Crime Agency of the UK, working in close cooperation with the FBI and the international law enforcement task force, 'Operation Cronos'.

We can confirm that Lockbit's services have been disrupted as a result of International Law Enforcement action – this is an ongoing and developing operation.

Return here for more information at:

11:30 GMT on Tuesday 20th Feb.

LockBit website seized

Your next steps

Challenge assumptions

"Humans are allergic to change. They love to say, 'We've always done it this way. ' I try to fight that. That's why I have a clock on my wall that runs counter-clockwise."

Rear Admiral Grace Hopper

- United States Navy Rear Admiral
- American computer scientist, mathematician
- Discovered the first computer “bug” in 1951

Most Cyber Secure Country

"As a nation, we cannot sleepwalk into our cyber future. I want Australia to be the world's most cyber secure country by 2030. I believe that is possible, but it will take a concerted effort from industry and Government alike."

The Hon Clare O'Neil MP

- Australian Minister for Home Affairs and Cyber Security
- Youngest female Mayor in Australian history
- Former McKinsey & Company consultant
- Fulbright Scholar

Help Australia become more secure by 2030

- Challenge assumptions holding cyber back
- Promote cultural change from the dev to board & senior leadership level
- CISOs must lobby for increased Cyber budget
- CISOs must report to CEO or the board
- Recognise we may be in a CyberWar already

Thank you for listening

Talk to me about
Data-breaches & Strategic Cyber Uplift

Andrew Horton

andrew.horton@threatcanary.io

0429 840 398