ARCTIC WOLF

THE LEADER IN SECURITY OPERATIONS

Security Operations in the Age of Cybercrime

Alex Pierce
Systems Engineer, Arctic Wolf

Today’s Speaker & Agenda

Alex Pierce
Systems Engineer
Arctic Wolf

01 How Big has Cybercrime Become?

02 Attack Method Examples

03 Recent Canadian Cyber Attacks

04 Meet the Threat Actors: Who to Look Out For

05 Why is this Important?

HOW BIG IS THE CYBERCRIME BUSINESS?

The $1.5 Trillion Dollar Cybercrime Industry

#1 Global Business Risk

Allianz Risk Barometer 2022 lists cyber incidents as the #1 global business risk, above business interruption and natural disasters.

Source: Allianz Risk Barometer 2022

$1 billion in Annual Revenue for Cybercriminals.

CyberSecurity Ventures, and ransomware attack statistics, reveal $1 billion in annual revenues for cybercriminals. That's a ransomware attack every 11 seconds by 2022.

Source: Bromium, Inc.

20x Greater Gains Compared to Largest CDN Company

Cybercrime totals $1.5 trillion in revenue annually. Brookfield Asset Management's revenue reached $75.7 billion in 2022. In comparison to Brookfield, cybercrime enjoys over 20x greater gains.

Source: Arctic Wolf

$8.4 Trillion in Annual Damages

Measured as a country, cybercrime would be the world's third-largest economy after the U.S. and China with inflicted damages totaling $8.4 trillion USD globally in 2022.

Source: Statista Technology Market Outlook, National Cybersecurity Organizations, FBI, IMF

Attack Method Examples

Ransomware as a Service (RaaS)

What is RaaS?
The commodification and commercialization of distributing ransomware to affiliate groups.

Attack Method
Ransomware developers work with affiliate groups that distribute their ransomware and then benefit economically from the attacks.

Business Email Compromise (BEC)

What is BEC?
The tactic of spoofing and taking over email addresses

Attack Method
BEC attacks can come in various forms – from attackers positioning themselves as the CEO requesting an emergency fund to acting company suppliers and requesting fund transfers to fraudulent accounts. BEC attacks target employees up and down the corporate ladder. It's reported 50% of companies will experience BEC

Zero-Day Exploit Market

What are Zero-Day Exploits?
Commercial activity that happens around the trafficking of software exploits.

Attack Method
Since Zero-Days are flaws or loopholes already present in the system in place, it makes the attack more reliable and sophisticated. They are undetected until the day they are released and therefore can be exploited while staying under the radar, which makes them highly effective for threat actors.

Recent Canadian Cyber Attacks

SickKids Hospital (December 2022)

What happened?
Ransomware

What was the impact?
Website, phonelines and internal systems affected.

Who was responsible?
Lockbit

Okanagan College (January 2023)

What happened?
Ransomware

What was the impact?
Classes disrupted, student records exfiltrated, systems down for extended period

Who was responsible?
Vice Society

Indigo (February 2023)

What happened?
Ransomware

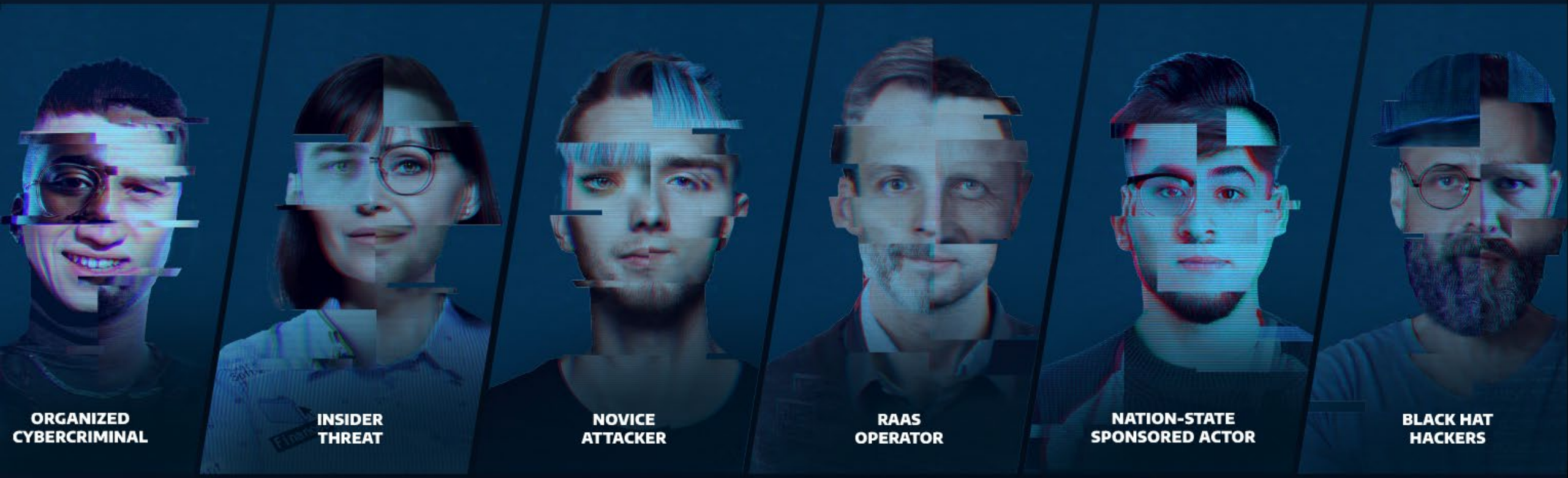
What was the impact?
Website and payment systems offline + personal identifiable information posted to the dark web

Who was responsible?
Lockbit

WHO TO LOOK OUT FOR

Meet the Players

While there are many cybercriminals out there, these are the 6 key threat actor groups to look out for that are trying to build their business and make money off your organization's mistakes.



Beware… Novice Attackers on the Rise!

LOW(ER) BARRIER TO ENTRY

ChatGPT, AI, accessible archives = access for lower, less technical skilled

MANY GATEWAY ACTIVITIES

Escalation paths for pre-career youth: e.g., game hacking to for-profit activity

SIGNIFICANT INCENTIVES

200K+ dark web job ads, peak salaries $15-20K/mo. for attack specialists

ALWAYS ON RECRUITMENT

Fewer constraints for malicious recruiters than legal businesses

"We see a lot of cybercrime born out of a lack of career options and socioeconomic issues in various places around the world."
-Christopher M Davis

Why Does this Matter & What Can I Do?

WHY IS THIS IMPORTANT?

Cybercrime is a Lucrative Industry

As long as there is money, attackers will continue to attack, grow their businesses and improve their strategies to siphon money from organizations.

How Much Money Is There?

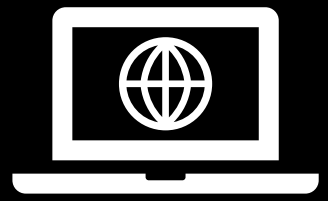
In 2022, data breach costs rose from $3.8 million to $4.2 million, the highest average total cost in the 17-year history of this report.

What Can I Lose?

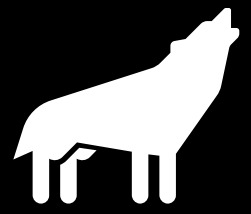
As cyber attacks continue to evolve, their direct and hidden, unexpected costs of data breaches continue to grow.

Stay Vigilant 24x7x365

Educate Your Employees



Monitor & Remediate Vulnerabilities



Partner with a Security Operations Provider

ARCTIC WOLF

THE LEADER IN SECURITY OPERATIONS

Questions?