FireEye
SECURITY REIMAGINED

REPORT

FIREEYE THREAT INTELLIGENCE

CYBER THREATS TO THE NORDIC REGION

MAY 2015

SECURITY REIMAGINED

CONTENTS

THE NORDIC REGION IS EXTOLLED FOR ITS RICH NATURAL RESOURCES, innovations in renewable energy and healthcare, and transparency in government. These traits also make the region a prime target of cyber threat groups. Threat actors have targeted strategic industries and government and defense agencies searching for valuable economic, political, and military intelligence. Their goal: capitalize on Nordic countries' robust economies and gain an upper hand in the region's distinct geopolitical concerns.

This report details some of cyber threat activity we have observed against Denmark, Finland, Iceland, Norway, and Sweden. We explore motivations of the cyber threat and factors that could trigger future activity in the region.

KEY FINDINGS

State-sponsored threat actors pose the greatest risk to Nordic governments and industries. These threat actors want state secrets, sensitive personal and financial data, and intellectual property from key industries. State-sponsored threat actors most likely seek to use any information that they obtain to benefit their government's decision makers and industries.

Nordic companies and governments are likewise vulnerable to cyber criminals looking to cash in on stolen data. Malware used in these attacks could pose an incessant burden to network defenders.

State-sponsored threat actors could conduct computer network attacks against strategic Nordic assets if tensions increase or conflict arises between the sponsoring government and victim country.

KEY SECTORS FACING CYBER THREATS

Nordic countries' robust aerospace and defense, energy, healthcare and pharmaceutical, shipping, and governments are prime targets for cyber threat actors in search of valuable economic, political, or military intelligence.

SECTOR	INTEREST OF ADVANCED PERSISTENT THREAT GROUPS	KEY INDUSTRIES
Aerospace and Defense	APT groups target and steal intellectual property and other sensitive data from regional aerospace and defense organizations.	■ Aerospace and defense manufacturing ■ Commercial space vehicles, rockets, satellites, aircraft ■ Science R&D ■ Military aircraft, missiles, rockets, satellites
Energy	The energy sector is a strategic industry, with implications for countries' economic development, military security, sovereignty, and political influence. This sector is particularly relevant in the Nordic region, given Norway's resources and role as a top supplier to the EU.	■ Oil and gas exploration, production and distribution ■ Green energy development ■ Industrial control systems
Healthcare and Pharmaceuticals	Multiple APT groups target this sector globally, most likely to obtain intellectual property to provide their own indigenous companies with an economic advantage. The Nordic region – Denmark in particular – is known for its innovations in the healthcare and pharmaceutical industry.	■ Pharmaceuticals ■ Biotechnology ■ Medical equipment ■ Hospitals ■ Healthcare providers ■ Health insurance
Shipping	The shipping industry probably faces threats from both APT groups and cyber criminals, given its economic importance and handling of valuable goods and equipment.	■ Shipping ■ Retail/delivery ■ Harbor/port management ■ Shipbuilding
Governments	APT groups frequently pursue governments and militaries to steal intelligence. Nordic countries' interests in the Arctic Circle and proximity to Russia make them targets for military and political espionage.	■ Foreign ministries ■ Militaries

THE NORDIC REGION

In the Crosshairs of Targeted Threat Actors

Table 1 lays out key economic and political risk factors for Nordic states. These strategic industries and geopolitical interests place commercial and government organizations in the crosshairs of targeted threat groups. We cannot definitively say if these threat actors work for their governments, but their operations are often aligned with their government's objectives.

Russia-based threat groups are known to target Nordic governments and industries that compete with Russia in the European energy market. Russia and its Arctic Circle neighbors have overlapping territorial claims and conflicting interests in the region.

China-based groups also have targeted Nordic countries. These groups are likely looking to steal economic information and intelligence about Nordic governments' plans and interests in the Artic. These include research, trade, and access to shipping routes and natural resources.

- Norway probably has the greatest risk of being targeted by China-based groups. Relations between Oslo and Beijing have been tense since 2010, when the Norwegian Nobel Committee awarded the Peace Prize to an imprisoned Chinese human rights activist. In 2012 and 2013, Norway considered blocking China's attempts to gain observer status in the Artic Council. And in January 2015, Norway expelled two Chinese students over national security concerns.[1]

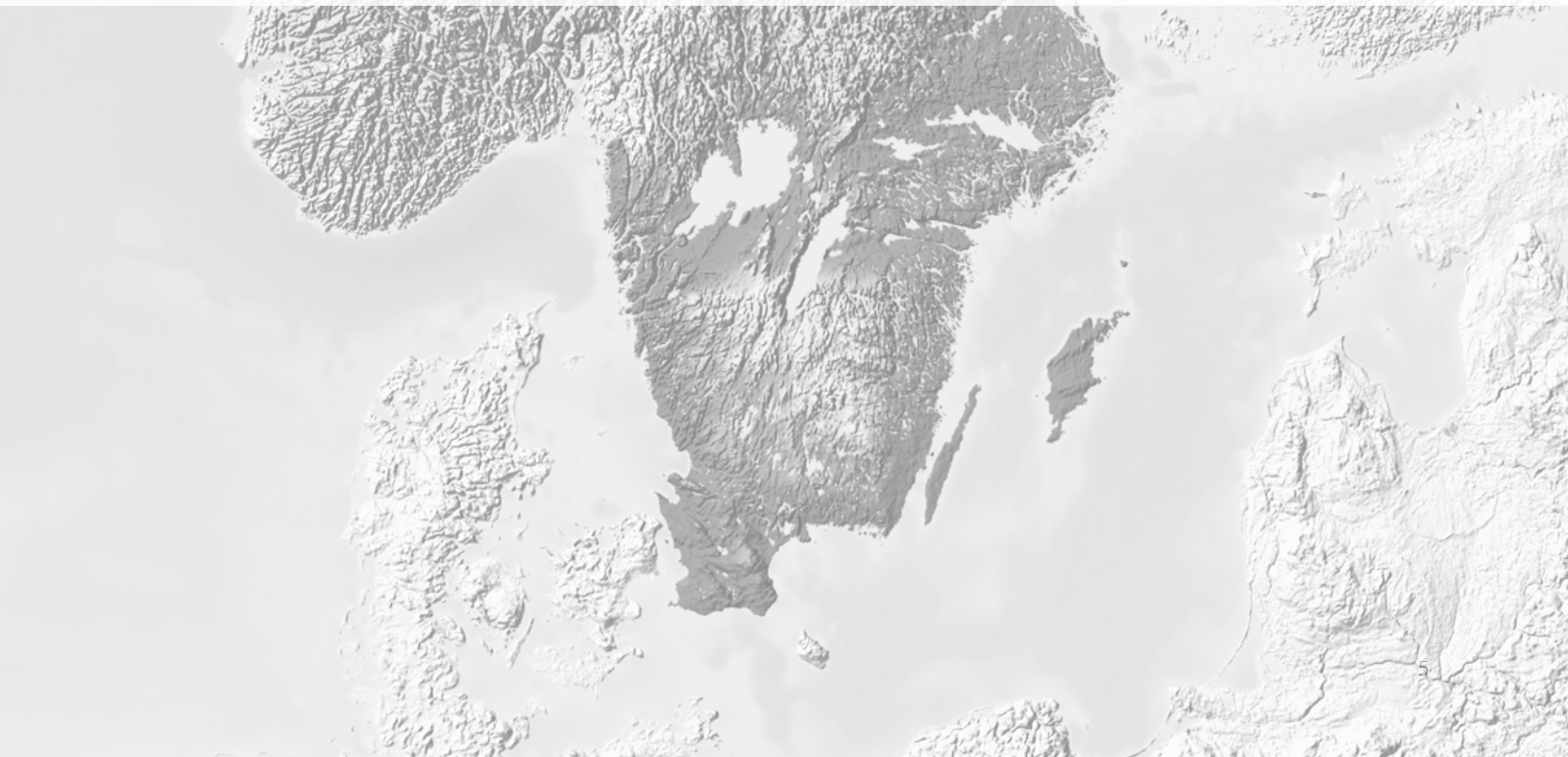

Table 1: Key Nordic Economic and Political Risk Factors

COUNTRY	DENMARK	FINLAND	ICELAND	NORWAY	SWEDEN
					
PARTICIPATION IN REGIONAL ORGANIZATIONS					
EU	X	X			X
NATO	X	Bilateral partner increasing participation in NATO operations amid Western tensions with Russia.	X	X	Bilateral partner increasing participation in NATO operations amid Western tensions with Russia.
OSCE	X	X	X	X	X
Arctic Council	X	X	X	X	X
KEY ECONOMIC TRAITS					
	Intellectual property, research and development, particularly in healthcare	High-tech innovations, telecommunications	High-tech and software development, biotechnology innovations	Oil and gas reserves, investment in renewable energy	Large manufacturing (cars, machinery, and industrial equipment)
SECURITY CONCERNS VIS-À-VIS RUSSIA					
	In March 2015, Russia suggested that Denmark's navy could become a nuclear target after Denmark proposed it would host NATO's missile defense shield on its frigates.[2] Denmark does not currently host the missile shield. Denmark and Russia also have conflicting territorial claims in the Arctic Circle.	Russia has grown increasingly concerned about Finland's cooperation with NATO and has reopened a military base near the Finnish border.[3] In response, Finland has sought to strengthen defense cooperation with Sweden, another non-aligned NATO partner that is not covered by Article V, NATO's mutual assistance doctrine.[4]	Iceland is the only NATO member without a standing military, and is reliant on its multilateral partners for defense.[5] Since 2007, Russian strategic bombers have flown occasional training sorties near Iceland's air defense zone.[6] In 2009 a cross-party parliamentary committee identified the rearmament of military forces in the Artic and cyber security as top security vulnerabilities.[7]	Norway has Europe's largest oil and natural gas reserves and is the EU's top energy supplier after Russia.[8] In a conflict, an adversary might attempt to disrupt Norway's production to cut off Europe's energy supply.	Sweden has contended with several recent instances of Russian aggression, including suspected submarine activity off its coast, an unannounced mock nighttime bombing raid over Stockholm, and repeated airspace violations.[9][10][11]

DETECTING THREAT ACTIVITY

Towards Our Nordic Clients

FireEye products continue to assist clients in the Nordic region to identify malware that advance persistent threat (APT) groups and other targeted actors use when attempting to access their networks. The statistics in this section are generated from clients that have opted to share anonymized data through the FireEye Dynamic Threat Intelligence (DTI) network. The data provides a glimpse into cyber threats facing the region.

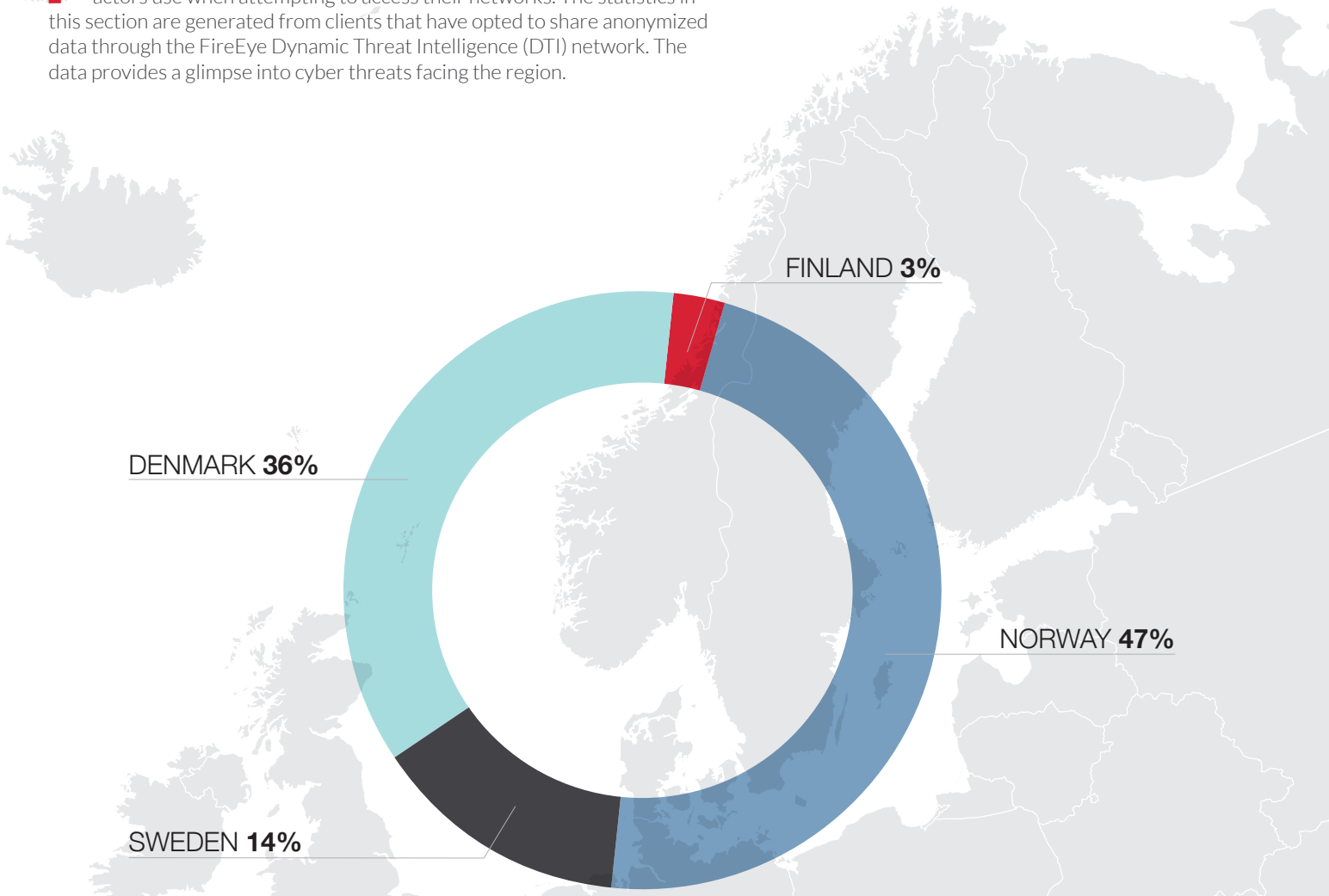

Figure 1: APT and Targeted Malware Alerts in the Nordics: Breakdowns by Country

Figure 2: APT and Targeted Malware Infections: Nordic Region

APT and Targeted Malware Targeting the Nordic Region

LV (NjRAT), XtremeRAT, and Gh0stRAT were the most prevalent malware families that FireEye products detected among our clients in the region. LV alone constituted half of targeted malware detections.

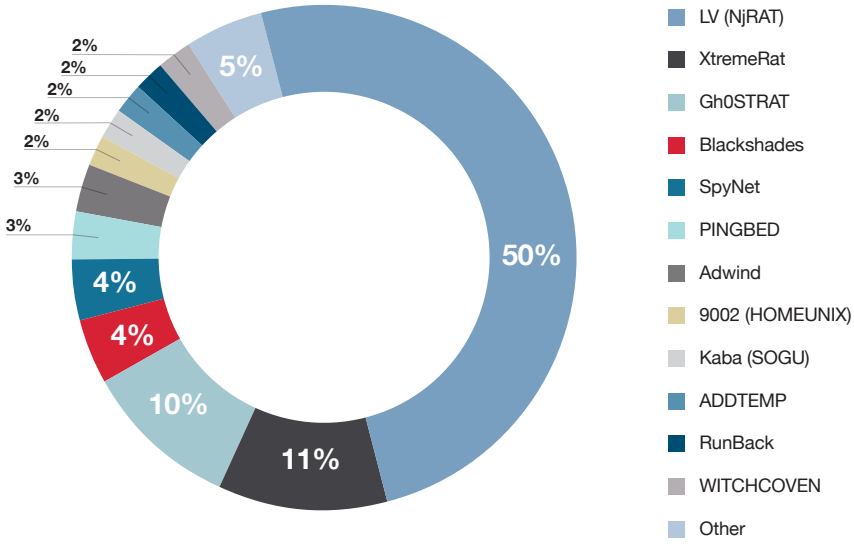

Figure 3: Targeted Malware Alerts By Industry: Nordic Region

Industry Breakdown of APT and Targeted Malware Alerts

More than a third of the APT and targeted malware FireEye detected originated from clients in the services and consulting sector. (Note: These statistics do not account for the number of appliances at a client site or the number of FireEye clients in a specific industry.)

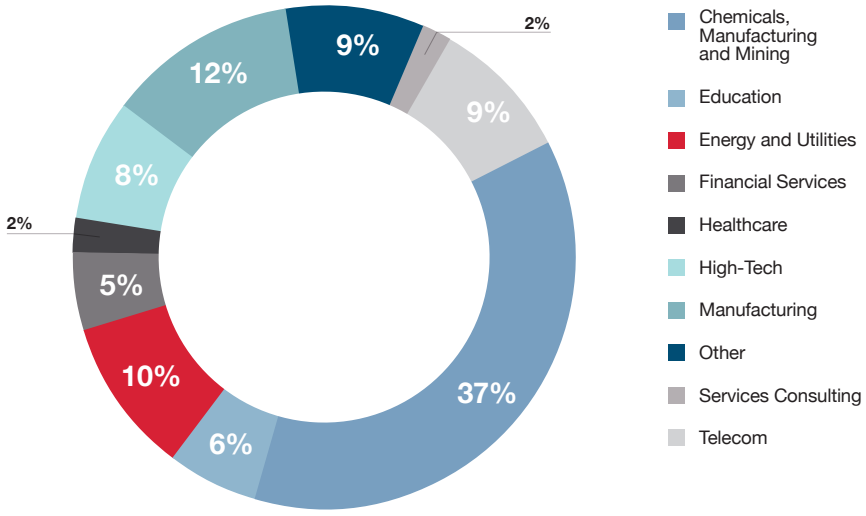

Figure 4: Crimeware Infections Among FireEye's Nordic Clients

Crimeware in the Nordic Region

Our Nordic clients also faced threat activity associated with cyber crime. Though distinct from APT group activity, cyber crime can still have serious ramifications. Crimeware variants—including botnets, Trojans, and ransomware—can consume an organization's computing power, steal and expose sensitive information, and enable financial theft.

Of the crimeware variants affecting our clients in the region, FireEye most frequently detected Zbot (Zeus), followed by Nymiam, Hardcore, and DarkComet, among others. The majority of the crimeware variants that we identified were so-called "infostealers" designed to collect credentials and other private user information.

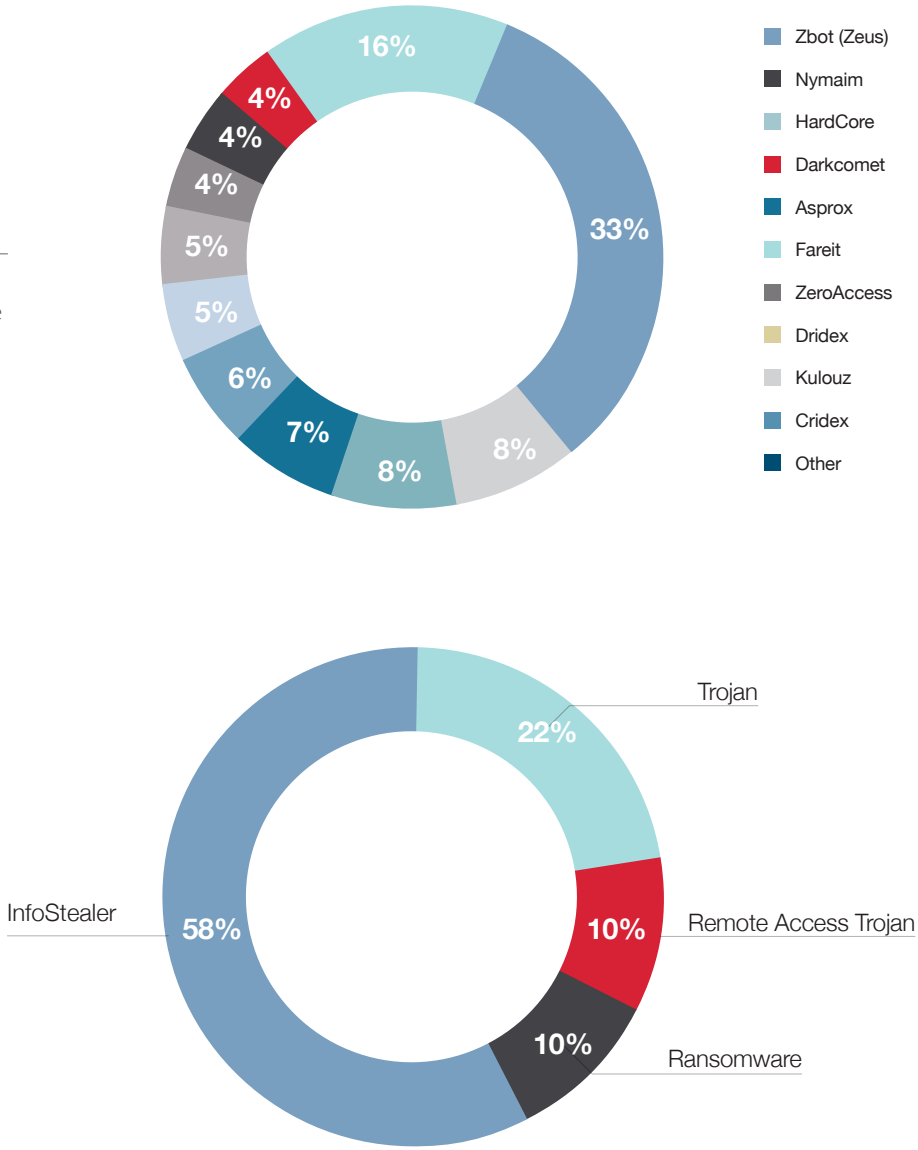

Figure 5: Types of Crimeware Prevalent Among FireEye Clients in the Nordic Region

TARGETING KEY INDUSTRIES
for Economic Espionage

Many times, we have investigated cases in which government-backed APT groups, particularly those from China and Russia, have compromised and stolen data from clients in the Nordic states.

These threat actors often target their victims' most sensitive information, including executive emails, financial data, and intellectual property. They probably hand the data over to support the sponsor government's economic, military, and political goals.

Governments can use this information to boost domestic industries. By stealing foreign competitors' goods and technologies, they can undercut competing suppliers on the global market and gain the upper hand in negotiations with foreign counterparts.

Table 2 highlights several regional industries we believe are particularly interesting to APT groups.

Table 2: APT Groups' Economic Interests and Likely Targets

SECTOR	INTERESTS OF APT GROUPS	RECENT CASES	MOST LIKELY CORPORATE TARGETS
Aerospace and Defense	APT groups target and steal IP and other sensitive data from aerospace and defense organizations in multiple countries. The sector is particularly valuable for state-sponsored actors, given its importance to Nordic military forces, defense industries, and global arms trade.	We investigated an incident in 2011 where a China-based threat group compromised the network of a Nordic aerospace equipment manufacturer. The group stole several file directories containing: ■ Corporate communications ■ Aerospace presentations ■ Sales, marketing, and facility-management information This group had already compromised and stolen data from numerous US defense firms and other victims.	■ Aerospace and defense manufacturing ■ Commercial space vehicles, rockets, satellites, aircraft, ■ Science R&D ■ Military aircraft, missiles, rockets, satellites
Energy	The energy sector is a strategic industry that greatly affects countries' economic development, military security, sovereignty, and political influence. This sector is particularly relevant in the Nordic region, given Norway's resources and role as a top supplier to the EU. Norway has sought to increase the amount of gas that it supplies to the EU and Baltic states amid concerns about their dependence on Russian energy following the crisis in Ukraine and resulting tension between Russia and Europe.[12] In providing an alternative to Russian gas, Norway is also undercutting one of Russia's key sources of leverage. The sensitivity surrounding this effort is not lost on Norway's police, who claim that Russia is increasing its intelligence collection with regards to Norway's energy sector, possibly for "sabotage purposes." [13]	In August 2014, Norway's National Security Authority (NSM) announced threat actors had compromised as many as 50 Norwegian oil companies, including its largest, state-owned oil firm Statoil. The NSM advised 250 other energy companies to check their networks for evidence of malicious activity. This activity affected several clients in the energy industry. In one case, threat actors sent a phishing email with a malicious attachment to a high-ranking employee in the procurement division at a Nordic energy company. The email purported to be from the company's human resources team and threatened the employee with dismissal. Threat actors also sent phishing emails to several other company employees, including two in the legal and procurement departments. These phishing emails appeared to be from human resources representatives and contained malicious PDF attachments. We believe this activity is associated with the suspected Russian actors behind the Fertger/Havex malware family, which other researchers refer to as "Energetic Bear" or "Dragonfly."	■ Oil and gas exploration, production and distribution ■ Green energy development ■ Industrial control systems

Table 2: APT Groups' Economic Interests and Likely Targets

SECTOR	INTERESTS OF APT GROUPS	RECENT CASES	MOST LIKELY CORPORATE TARGETS
Healthcare and Pharmaceuticals	The Nordic region – Denmark in particular – is known for its innovations in the healthcare and pharmaceutical industry.[14] We have seen multiple APT groups target this sector globally – most likely to obtain intellectual property to provide their own indigenous companies with an economic advantage. The industry is also emerging as a prime target for both state actors and cyber criminals looking to steal personally identifiable information. Just this past year, several American healthcare providers suffered high profile breaches resulting in the large-scale theft of patient information.	The high level of digitalization in the region—Denmark and Sweden rank among the highest in terms of Internet connectivity and integration of the EU countries – has raised concerns about the security of citizens' sensitive data, and permission for its collection.[15] [16] In 2014, the Danish public became aware of a government-mandated healthcare data collection program compiling citizens' sensitive medical data in a privately hosted database available to publicly and privately funded researchers.[17] The ensuing controversy highlighted the public's unease about the collection of sensitive data, as well as concerns over its security. While accidental exposures of such data most likely will embarrass and threaten the privacy of those affected, threat groups may also attempt to steal such data for identity theft (including medical identity theft), or to profile patients, or facilitate other targeting and espionage efforts.	■ Pharmaceuticals ■ Biotechnology ■ Medical equipment ■ Hospitals ■ Healthcare providers ■ Health insurance
Shipping	The shipping industry probably faces threats from both APT groups and cyber criminals, given its economic importance and handling of valuable goods and equipment. APT groups have compromised shipping companies in the past, stealing: ■ Blueprints for new ship models ■ Internal emails ■ Financial records ■ Files related to business plans, production, sales, and services Cyber criminals have also targeted shipping records to facilitate the theft or transport of illegal cargo.	Nordic shipping companies would most likely be at risk of financial loss and reputational damage as a result of cyber criminal activity. A shipping company experienced a similar situation in 2013 at a port in Antwerp, Belgium, when police found that international drug cartels had used cyber criminals to breach the company's networks to help them send and receive illegal drugs.[18] The cyber criminals used their access to alter shipment records and obtain security codes for retrieving the cargo from the port. Belgian and Danish police estimate that this activity helped the cartels transfer as much as two tons of cocaine and heroin during a two-year period.	■ Shipping ■ Retail/delivery ■ Harbor/port management ■ Shipbuilding

THREATENING NORDIC ORGANIZATIONS

That Promote Transparency and Free Speech

We have frequently observed these actors stealing data, which the sponsoring government most likely uses to monitor activities it perceives as controversial or sensitive.

Efforts to promote free speech and transparency probably makes Nordic nonprofits, minority groups, and media agencies a target of APT groups, whose sponsoring governments view those issues as a threat to their legitimacy and domestic stability.[19] We have frequently observed these actors stealing data, which the sponsoring government most likely uses to monitor activities it perceives controversial or sensitive.

Russia-based APT Group Conducts DDoS Attack on Controversial Chechen News Site

For several years, a Swedish Internet service provider hosted The Kavkaz Center, a controversial Chechen news site that critics claim promotes extremism. The Russian government tried to pressure Sweden into taking the site offline, and threat actors have targeted the site.

Over the course of two months in 2012, threat actors launched sustained distributed denial-of-service (DDoS) attack. In 2002, Kavkaz spokespersons alleged the Russian government was involved in taking the site offline during security forces' highly controversial Moscow theater raid in 2002.[20]

Hacktivists Protesting Cartoon Depiction of Muhammad Deface Danish Websites

In 2006, a Danish newspaper printed a controversial cartoon that critics said insulted the Prophet Muhammad.[21] In response, hacktivists defaced an estimated 1,000 Danish websites with messages condemning the image and its publication. Firms monitoring the defacements stated that individuals, some from as far as the Middle East and Asia, coordinated their activity through online forums.[22] Many of the affected sites belonged to smaller companies vulnerable because of their limited security awareness and resources.[23]

STEALING NORDIC COUNTRIES' POLITICAL and Military State Secrets

China-Based APT Group Uses Spear Phishing Emails Referencing Putin to Collect Diplomatic and Military Intelligence

In mid-March 2015, a China-based APT group sent spear phishing emails to Nordic security and defense organizations. The threat group used lures referencing Russian President Vladimir Putin's then-recent absence from public view, an event that had prompted media speculation over the state of his health and hold on power. [24]

The emails contained Word documents—one containing a news article from a UK newspaper—exploiting the CVE 2012-0158 vulnerability. It dropped a newly compiled variant of a malware family popular among known and suspected China-based threat groups.

This activity most likely was part of an effort to collect diplomatic and military intelligence.

Finnish Ministry of Foreign Affairs Reports Multi-Year Cyber Espionage Campaign

Finland's Ministry of Foreign Affairs announced in November 2013 that it had been the victim of cyber espionage and data theft of political intelligence for approximately four years.[25] The Finnish Foreign Minister notified other EU states, which the Minister said had encountered similar cyber espionage activity.

According to another Ministry official, the activity in Finland was "similar to, and more sophisticated" than the Red October cyber espionage campaign, which reportedly has been targeting similar data from European governments since 2007.[26]

Finland's official statement did not identify any suspects. But some security analysts speculate that Russian or Chinese actors were behind the activity.

Russia–Based APT Group Appears to Target Nordic Country's Military

In October 2014, we released a report on APT28,[1] a suspected Russian threat group that has systematically targeted Western and European governments and military organizations, including a military in the Nordic region.

APT28 primarily relies on phishing emails and spoofed login pages to collect credentials and compromise victims. The group has also been observed using zero-day exploits.

We believe this group seeks political and military intelligence, which it steals from its victims through implants configured to send data out of the network.

APT28 often tries to mask its activity from network administrators by using spoofed domains that mimic those of legitimate websites web users at the targeted entity would normally visit. For example, one of APT28's spoofed domains mimicked a website belonging to a Nordic country's military, suggesting that this military was one of APT28's targets.

[1] APT28 – A Window Into Russia's Cyber Espionage Operations is available at https://www2.fireeye.com/apt28.html.

TARGETING THE NORDIC ENERGY INDUSTRY

for Destructive Activity and Computer Network Attack

Espionage is not the only concern facing organizations in the Nordic region; organizations may also be at risk of politically motivated destructive activity or computer network attacks. This concern is particularly relevant for the energy industry, whose strategic importance makes it a target for destructive actors worldwide.

Norway is a top energy supplier for the EU and has publicly warned of potential threats from state actors. Ongoing tensions between Russia and the West over Ukraine have underscored Russia's control of Europe's energy supply and its ability to disrupt it.

In the past year, researchers identified two malware families that suspected Russian actors have used to target critical infrastructure in the Nordic region.

Norway's NSM officially stated that the Havex/Fertger malware found in the networks of Norwegian oil companies were most likely part of an espionage operation. But the threat actors may well have been conducting reconnaissance for later destructive activity.[27]

In February, Kaspersky Labs reported on another suspected Russian tool, BlackEnergy2, found on industrial control system (ICS) networks, including that of an organization in Sweden.[28 29] The malware can overwrite data and was most likely intended for sabotage.

EYEING NORDIC HEALTHCARE
and Personal Information for Cyber Crime

Enterprise–like cyber criminal groups also go after Nordic organizations and steal data for financial gain.

APT groups are not the only threat actors eyeing potential victims in the region. Enterprise–like cyber criminal groups also go after Nordic organizations and steal data for personal gain.

These threat actors search for data they can easily monetize, such as personally identifiable information or financial account data. Some actors use this stolen information to steal victims' identities, withdraw funds, and make fraudulent purchases. Others sell the information on underground markets.

In addition to potential threats to healthcare and personal information, cyber criminals pose a threat to other Nordic industries.

In one case, we found three different types of crimeware in the network of an industrial equipment manufacturer. During an investigation at a telecommunications company, we found that threat actors had tried to change server routing tables, most likely to leverage the firm's infrastructure for further operations.

CONCLUSION

Nordic organizations will face persistent threats because of the region's strong industries, intellectual property, insider data, and geopolitical interests. While we anticipate that Nordic countries will experience mostly consistent threats, certain events may trigger spikes in activity.

For example, threat actors engaged in economic espionage most likely will increase their targeting activity against organizations that have identified a potentially lucrative new innovation. They might seek to steal designs for a newly developed product. Or they may want to gain the upper hand for their sponsor in trade deals or negotiations.

Threat actors searching for political and military intelligence, in turn, will almost certainly increase their targeting tempo during strategic negotiations or increased tension between their sponsor and targeted government.

Geopolitical tensions, such as Arctic territorial disputes, NATO operations, and the ongoing crisis in Ukraine, will most likely influence targeting as rival parties seek to advance their goals with valuable intelligence. And if tensions escalate—or devolve into outright conflict—organizations in the Nordic region may also be at an increased risk of destructive activity or computer network attacks meant to damage or destroy key infrastructure.

APPENDIX A
ENDNOTES

1 Baker, Benjamin David. "From China with Love: China, Norway, and Espionage." The Diplomat. 14 Feb. 2015. Web. 14 April 2015.

2 "Russian Ambassador Warns Denmark Over NATO Missile Shield." Agence France-Presse via Defense News. 22 March 2015. Web. 25 March 2015.

3 Bender, Jeremy. "Russia is Constructing an Arctic Stronghold 30 Miles from the Finnish Border." Business Insider. 14 Jan. 2015. Web. 25 March 2015.

4 Harress, Christopher. "Scared by Russia, Sweden and Finland Make War Pact." International Business Times. 19 Feb. 2015. Web. 25 March 2015.

5 "U.S. Relations with Iceland."Bureau of European and Eurasian Affairs, U.S. Department of State. 21 Jan. 2015. Web. 13 April 2015.

6 Benedictsson, Einar. "At Crossroads: Iceland's Defense and Security Relations, 1940-2011." US Army Strategic Studies Institute, the US Army War College.18 August 2011. Web. 11 May 2015.

7 Summary of the Findings of an Interdisciplinary Commission Appointed by the Icelandic Foreign Minister. "A Risk Assessment for Iceland: Global, Societal, and Military Factors." Icelandic Ministry of Foreign Affairs. March 2009.

8 "Norway can 'Slightly Boost' Gas Supply to EU." The Local. 26 Sept. 2014. Web. 12 March 2015.

9 Nordenman, Magnus. "Sweden's Mysterious Submarine Hunt and its Significance for Nordic-Baltic Security." The Atlantic Council. 20 Oct. 2014. Web. 25 March 2015.

10 Cenciotti, David. "Russia Simulated a Large-Scale Aerial Night Attack on Sweden." Business Insider. 23 April 2013. Web. 12 April 2015.

11 Mohsin, Saleha. "Russia Threat Prompts Nordic Governments to prepare for Worst."15 Nov. 2014. Web. 11 March 2015.

12 "Norway can 'Slightly Boost' Gas Supply to EU." The Local. 26 Sept. 2014. Web. 12 March 2015.

13 "Norway Intelligence Claims Russian Intelligence Intensifies Monitoring Norwegian Energy Activities." The Nordic Page. 24 March 2015. Web. 24 March 2015.

14 "The Pharmaceutical Market: Denmark." Espicom, Business Monitor International. 20 Dec. 2014. Web. 25 March 2015.

15 "Denmark." Digital Agenda for Europe: A Europe 2020 Initiative. European Commission. 24 Feb. 2015. Web. 21 April 2015.

16 "Sweden." Digital Agenda for Europe: A Europe 2020 Initiative. European Commission. 24 Feb. 2015. Web. 21 April 2015.

17 Degett, Jens. "One Step Too Far for Legendary Danish Transparency." EuroScientist. 25 March 2015. Web. 21 April 2015.

18 Pasternack, Alex. "To Move Drugs, Traffickers are Hacking Shipping Containers." Motherboard, Vice. 21 Oct. 2013. Web. 2 April 2015.

19 Tatlow, Didi Kristen. Smale, Alison. "China Loses Ground in Transparency International Report on Corruption." The New York Times. 3 Dec. 2014. Web. 20 April 2015.

20 Sturgeon, Will. "Russia accused of waging cyber-war on Chechnya." ZDNET. 14 Nov. 2002. Web 30 April 2015.

21 Ward, Mark. "Anti-Cartoon Protests Go Online." The BBC. 8 Feb. 2006. Web. 30 April 2015.

22 Ward, Mark. "Anti-cartoon protests go online." The BBC . 8 Feb. 2006. Web. 30 April 2015.

23 Ward, Mark. "Anti-cartoon protests go online." The BBC . 8 Feb. 2006. Web. 30 April 2015.

24 Keating, Joshua. “Putin is Back! Gives No Explanation for His 10-Day Disappearance.” Slate. 16 March 2015. Web. 9 April 2015.

25 Pohranpalo, Kati. Viita, Kasper. “Finland Probes Hacking of Foreign Ministry Network.” Bloomberg LP. “1 Nov. 2013. Web. 9 April 2015.

26 Farivar, Cyrus. “Finland’s Foreign Ministry Gets Pwned by Worse-Than-Red October Malware.” Ars Technica, Conde Nast. 31 Oct. 2013. Web. 9 April 2015.

27 “Hackers attack Norway’s oil, gas, and defence business.” The BBC. 18 November 2011. Web. 30 April 2015.

28 Baumgartner, Kurt. Garnaeva, Maria. “BE2 Extraordinary Plugins, Siemens Targeting, Dev Fails.” Securelist. Kaspersky Labs. 17 Feb. 2015. Web. 10 April 2015.

29 Baumgartner, Kurt. Garnaeva, Maria. “BE2 custom Plugins, Router Abuse, and Target Profiles.” SecureList. Kaspersky Labs. 3 Nov. 2014. Web. 9 April 2015.

To download this or other
FireEye Threat Intelligence reports,
visit: https://www.fireeye.com/reports.html

FireEye, Inc. | 1440 McCarthy Blvd. Milpitas, CA 95035 | 408.321.6300 | 877.FIREEYE (347.3393) | info@fireeye.com | **www.fireeye.com**