ANOMALI

Cyber Threat Landscape North America

Source Summary Statement: *This product is based on research utilizing various open and private sources, proprietary sources, and intelligence vendors. This Cyber Threat Landscape report is based on collections and analysis that ended 02 OCT 2020.*

Overview

Anomali Threat Research conducted an analysis of numerous types of malicious cyber activity affecting North America. Due to the complex nature of sophisticated threat actors and groups, in addition to economic and geopolitical factors that can motivate cyberattacks, this report will be broken down into specific sections to highlight specific threats and risks. The most prolific threat groups and most-observed tactics, techniques, and procedures (TTPs) that are being used by threat actors will be discussed, as well as current geopolitical topics that contribute to and affect malicious cyber activity.

North America

The following countries and territories are considered part of North America for the purposes of this report. Countries: Antigua and Barbuda, Bahamas, Barbados, Belize, Canada, Costa Rica, Cuba, Dominica, Dominican Republic, El Salvador, Grenada, Guatemala, Haiti, Honduras, Jamaica, Mexico, Nicaragua, Panama, Saint Kitts and Nevis, Saint Lucia, Saint Vincent and the Grenadines, Trinidad and Tobago, United States of America (US). Territories: Anguilla (UK), Aruba (Netherlands), Bermuda (UK), Bonaire (Netherlands), British Virgin Islands (UK), Cayman Islands (UK), Clipperton Island (France), Curacao (Netherlands), Greenland (Denmark), Guadeloupe (France), Martinique (France), Montserrat (UK), Navassa Island (US), Puerto Rico (US), Saba (Netherlands), Saint Barthelemy (France), Saint Martin (France), Saint Pierre and Miquelon (France) Sint Eustatius (Netherlands), Sint Maarten (Netherlands), Turks and Caicos Islands (UK), US Virgin Islands (US).

Geopolitics

As former colonies of France, Spain, and the UK (among copious other societal and cultural influences), Canada, Mexico, and the US share numerous cultural outlooks and languages. Canada and the US have close government ties as members of the Five Eyes (FVEY) intelligence alliance, which also includes Australia, New Zealand, and the United Kingdom. This intelligence alliance was sparked by the joint declaration made in 1941 called The Atlantic Charter, later instituted in the United Kingdom — United States of America Agreement (UKUSA) signed by President Franklin Roosevelt and Prime Minister Winston Churchill for objectives after the end of World War II.[1] Interestingly, while Mexico, Canada, and the US have close relations in some areas, Mexico is not a member of FVEY. This arrangement provides Canada and the US with effective cyber intelligence sharing from each of the partners' Signals Intelligence (SIGINT) but increases the potential for state-sponsored groups to target either country for strategic objectives. These are inherent risks of partnership, as adversaries know that specific entities hold valuable intelligence and will thus attempt to exploit weaknesses in one partner to compromise another (similar to a supply-chain attack). State-sponsored advanced persistent threat (APT) groups are often motivated by theft of this type of information. Canada and the US also share membership in the North Atlantic Treaty Organization (NATO), and the countries' militaries operate together within the North American Aerospace Defense Command (NORAD).[2] NORAD was officially instituted on May 12, 1958 and can be traced back to post World War II cooperation between the US and Canada. Cooperation continued post-World War II with the mutual desire for defensive network capabilities due to a Europe, the Korean War, and increasing Soviet Union military capabilities, amongst the other strategic interests.[3]

The region's largest economies, Canada, Mexico, and the US, have been disputing a variety of issues such as immigration and trade. Canada and the US are both each other's largest trading partners, and the US is also Mexico's primary trading partner.[4] In addition, Mexico is the US' second-largest trading partner and Canada's fifth, as of 2019.[5] Furthermore, Canada and the US share the world's largest international border that had 94,662,104 crossings in 2019.[6] The US and Mexico share one of the most heavily traveled borders, with 275,538,145 crossings in 2019.[7] In FY 2019, goods valued at $2.67 trillion (USD) crossed into the US from Mexico.[8] The high traffic at the border, in addition to strategic entry points, represent value and profit for the Mexican drug cartels. The competing interests of drug traffickers and law enforcement sometimes results in violence, however, COVID-19 and subsequent border crossing limitations have caused cartels to amass their illicit supplies and wait out the pandemic.[9] The issues arising at the border have caused strains on the Mexico-US relations, particularly when nine US citizens were killed in Mexico in November 2019. That event caused US President Trump to offer his counterpart President Andrés Manuel López Obrador US intervention in Mexico, in addition to potentially labeling the cartel groups as terrorist organizations.[10] The offer was subsequently rejected by Obrador, and the border continues to be a common point of tension between Mexico and the US.

The strong trading and geographical ties have also been tested in different ways over the past several years, with US President Trump challenging and subsequently ending the North American Free Trade Agreement (NAFTA).[11] Canadian, Mexican, and US officials replaced NAFTA with an updated version of the trio trade-arrangement called the United-States-Mexico-Canada Agreement (USMCA), which went into effect July 1, 2020.[12] The agreement was very likely a welcome accord after President Trump threatened the US' largest trading partners with tariffs prior to the arrangement, to which Canada and Mexico responded with tariffs of their own.

The threatening rhetoric from President Trump not only caused disagreements among close trading partners and neighboring countries, but also extended to other countries and regions around the world.[13] Trump stated in February 2020, "Europe has been treating us very badly. Over the last 10, 12 years there's been a tremendous deficit with Europe."[14] Despite the heated words, the US and the European Union (EU) were able to reach an agreement that reduced tariff increases in late August 2020.[15] The resolution allowed the EU and US economies, whose trade relationship accounts for approximately half the world's GDP, to resume the low average tariff they typically employ.[16] While the EU and the US reached an arrangement, the US-China relations have not had such an outcome, and new retaliatory tariffs have happened somewhat frequently. As of this writing, the US has added new tariff exclusions on Chinese products on various goods, such as smart watches and some kinds of medical masks, until the end of 2020.[17] Previous US-China tariffs were at 15% in September 2019, and lowered to 7.5% via China's Phase 1 agreement signed in January 2020.[18] The four-month extension is different than previous one-year extensions implemented by the Trump administration, and it creates ambiguity for importers.

At the time of this report, China and the US were also negotiating the sale of the social media app TikTok's US division, after President Trump declared national security concerns with TikTok and WeChat, another Chinese-owned social media platform. President Trump gave TikTok's parent company, ByteDance, 45 days to sell all of their US assets or the app would be banned; the 45 days were extended when a Washington D.C. federal judge blocked the Trump administration's attempt to ban downloading TikTok in the US.[19] This act will give US-based companies Oracle and Walmart more time pursue purchasing of TikTok's US-based assets.[20] Security concerns with TikTok are well justified, as researchers have analyzed the app and have found that it can be utilized by actors to conduct multiple kinds of malicious activity. This malicious activity includes: cross-site scripting, cross-site forgery request, data exposure, and SMS link spoofing.[21] The TikTok code is likely still abusing permissions on installed devices and collecting sensitive information. In addition, the news of potential banning of the app increased the creation and subsequent distribution of fake, malicious TikTok apps.[22] Furthermore TikTok was banned by numerous entities around the globe, some of which include: Amazon, Wells Fargo, multiple branches of the US Armed Forces, the US Transportation Security Administration, the Indian government, and is being considered for banning by many others.[23]

Canadian and Mexican relations with the world's second-largest economy are starkly different in comparison. Canadian and Chinese relations have been bitter since December 2018, when Meng Wanzhou, the CFO of Huawei Technologies, was arrested at Vancouver International Airport on her way to Mexico from Hong Kong. The arrest was initiated at the request of the US who charged Wanzhou and two Huawei affiliates (Huawei Device USA and Skycom Tech) with conspiracy to defraud the US, financial fraud, and money laundering.[24] Wanzhou is currently under house arrest in Vancouver, fighting extradition to the US in the Canadian courts at the time of this writing.[25] Prior to this incident, Canada and China enjoyed approximately 50 years of ever-improving trade relationships, and in 2016 Chinese Premier Li Keqiang said he was looking forward to "a new golden decade" for the two countries.[26] While international relations between the countries have grown bitter, Canada was still China's second-largest trading partner in 2019.[27]

In contrast to its largest trading partners, Mexico has enjoyed stable relations with China, and even extended attempts for future economic and trading agreements.[28] Even after the USMCA agreement was signed, China and Mexico continued to pursue economic ties.[29] In February 2020, local reporting in Mexico stated at least 10 China-based companies attempt to move to Mexico every month.[30] In August 2020, President Xi Jinping and President Andrés Manuel López Obrador had a phone conversation in which Obrador thanked Jinping for the sale of medical equipment to combat COVID-19, to which Xi pledged additional support.[31] In addition, Mexico is located in a strategic position in the Western hemisphere, as both countries realize the potential advantages of a relationship to counter the Trump administration's "America First" rhetoric.

Cyber Landscape

The North American cyber threat landscape is largely-dominated by US-based activity. There are seven Computer Emergency Response Teams (CERTs) in the region, based in Canada, the Caribbean / Curacao, Dominican Republic, Guatemala, Mexico, Panama, and the US respectively.[32]

The continent boasts a robust cybersecurity market with an estimated value of $24.62 billion (USD) in 2015 that was projected to reach $53.34 (USD) by 2020 based on a Compound Annual Growth Rate (CAGR) of 16.73% over that time period.[33] The significant monetary value will almost certainly be a major factor for financially-motivated Advanced Persistent Threats (APTs) and threat groups to engage in malicious activity. Overall, the region has a robust cybercriminal and threat actor community that actively engages in malicious activity, primarily credit card theft and fraud, phishing, and ransomware attacks. Of particular importance, the United States represented 38.6% of the world's credit card fraud as of 2018, much of it cyber-enabled. The apparent steady rise in cyberattacks has not gone unnoticed by governments, and the USMCA agreement touches on numerous digital topics.

USMCA protects companies from releasing source code to enter a certain market, and also requires parties to agree to NIST cybersecurity policies.[34] There are also data-protection principles that require participants to publish information on how personal information is protected.[35] Regarding how this information is shared across borders, USMCA uses the APEC Cross Border Privacy Rules as an example of how to share data securely.[36] These provisions stated in the USMCA agreement includes important building blocks for present and future agreements for these three countries.

In addition to mutual agreements, numerous countries throughout North America have also developed and implemented independent cyber, communication, and information security policies. Economic size is often tied to the ability to provide funding for such projects, and many of the smaller and island countries have cooperated with delegations from the Organization of American States (OAS) to assist in creating said security policies.[37] With threat actors constantly changing their TTPs, having policies in place to adapt to these changes is a crucial step in preventing malicious activity.

While the COVID-19 pandemic has brought unprecedented changes to our society and economy, the effects on the cyber threat landscape have remained relatively minor.[38] Some of the changes in the cyber threat landscape post-COVID-19 include:[39]

- A shift from working in the office to remote locations exposes enterprise networks to a new type of threat.
- The use of COVID-19 topics and an increase in health-themes for social engineering.

Increase in the targeting of entities working in healthcare and healthcare-related manufacturing with cyberespionage objectives. In addition, these critical organizations are also increasingly vulnerable to ransomware attacks.

Threat Actors and Groups

There are multiple active and historic APT groups and threat actors that target entities and individuals with various motivations and objectives. A larger list of threat groups that target, or are located in, North America can be found in Appendix A. Awareness of these actors and their TTPs can assist in a proactive, rather than reactive, cyber strategy.

APT29

The Advanced Persistent Threat (APT) group "APT29" (Cozy Bear, Cozy Duke, Mini Duke, The Dukes) is a Russian-based group that was first reported on in July 2013 by Kaspersky and CrySyS Lab researchers.[40] The group boasts an arsenal of custom and complex malware at its disposal and is believed to be sponsored by the Russian Federation government. APT29 conducts cyber espionage campaigns and has been active since at least 2008. The group primarily targets government entities and organizations that work in geopolitical affairs around the world, however, a plethora of other targets have also been identified.[41]

APT29 is a highly-sophisticated group that employs a variety of tactics to accomplish their malicious objectives. Similar to other APT groups, APT29's primary initial infection is spearphishing; APT29 will also wrap its malware with legitimate applications for distribution. These spearphishing emails are crafted with information gathered from legitimate locations that would be relevant to the target recipient. For example, the group was found to use news articles and paste the content into Microsoft Word document attachments with malicious macros. Enabling of the macro begins the infection process for one of the numerous APT29 malware; typically the first infection is a backdoor, such as HammerToss, or a toolset, such as CosmicDuke. APT29 backdoors often have the ability to download a secondary backdoor, such as POSHSPY, to provide redundancy for continued access to an infected machine if a first-stage backdoor, such as PowerDuke, is discovered.[42]

APT41

APT41 is a China-based group that has carried out financially-motivated attacks from as early as 2012 but have become more known for their state-sponsored campaigns with activity as early as 2013.[43] The groups earliest activity focused on financial gain and would target organizations in the video game industry by gaining access to game development environments.[44] The groups' financially-motivated activities focused on stealing source code and digital certificates, virtual currency gold mining, and attempting to deploy ransomware within these game environments.[45] The TTPs used and campaigns carried out by APT41 for financial motivations have later been leveraged for state-sponsored attacks for China.[46] From 2013 onwards, APT41 has been observed to concurrently conduct cyberespionage operations against high-value industry sectors with their previous financially-motivated attacks towards the games industry.[47] The TTPs used by APT41 in their earlier financially-motivated attacks, such as stealing digital certificates to implant their malware into the systems of various organizations, have later been utilized in their state-sponsored campaigns.[48]

APT41 is a sophisticated group that utilizes a wide selection of custom malware and open-source tools to carry out their campaigns. APT41 primarily uses spearphishing emails, often with compiled HTML (.chm) attachments as the initial point of compromise.[49] Other infection vectors include leveraging stolen credentials and using legitimate digital certificates to sign malware for it to be deployed into the users systems.[50] The use of compiled HTML attachments makes the malicious program appear as legitimate by using a genuine Microsoft file format. The group sometimes uses legitimate documents and content in their spearphishing emails.

As an example, in 2015, a Japanese media organization was targeted with a lure document that translated to, "Prevention of Middle East Respiratory Syndrome (MERS)."[51] APT41, similar to other APT groups, utilize current and relevant themes to make spearphishing emails appear more legitimate..

Charming Kitten

The cyberespionage group "Charming Kitten" is believed to be an Iran-based group that has been active since at least 2014.[52] Charming Kitten conducts cyber espionage operations on many entities, particularly diplomatic, media, and military organizations. The group is known for creating fake social media profiles, to use in an attempt to social engineer their targets. Charming Kitten also creates multiple fake news outlets that copy news articles from other legitimate sources to use as a platform for attacks. The group has been observed to use gathered information to blackmail certain targets.

Charming Kitten utilizes multiple initial vectors to compromise a target. The group conducts large-scale phishing campaigns, distributing thousands of emails to hundreds of targets. Additionally, Charming Kitten will compromise email accounts of individuals whom the higher-profile targets may trust to send emails from that email address. For credential gathering, the emails contain links to a phishing site that masquerades as a Gmail shared document that "requires" the target to log into their Gmail account to view the document, thus stealing credentials. In other cases, the phishing site impersonated a Google Hangouts invite which required the user to login to join a conversation.[53] Finally, Charming Kitten has been observed sending spearphishing emails with the "DownPaper" Backdoor Trojan as an attached malware.[54]

Equation Group

The Equation Group is believed to be a US-based APT group discovered by Kaspersky researchers in a report published in 2015.[55] The group, believed to have been active since 2001, is highly sophisticated. Equation Group primarily targets entities located in the Middle East with custom and complex malware.[56] Equation Group uses numerous forms of encryption during their operations, and is associated to the Stuxnet worm based on numerous similarities to the group's custom "Flame" malware framework and the notorious malware.[57]

Equation Group is assessed to be capable of developing and maintaining sophisticated malware and conducting complex attacks. These attacks have taken shape in exploits (sometimes zero-days), physical media, and web-based exploits.[58] The group is patient and uses multiple layers of infection utilizing custom malware and tools, such as the Gauss malware platform and DoubleFantasy plugin, before moving forward with later stages of infection, such as the EquationDrug installer.[59]

TA505

The financially-motivated threat group called "TA505" was first reported by Proofpoint researchers in December 2017. Malicious activity attributed to the Russian-speaking group dates back to at least 2014, and the campaigns conducted by TA505 have targeted entities and individuals around the world. The group distributes a variety of malware, including well-known strains (Dridex banking trojan, Locky ransomware), custom-created (Jaff ransomware, tRAT), and variants of legitimate remote access tools (Remote Manipulator System). The group primarily distributes malware and tools via large scale and indiscriminately-distributed malspam campaigns, often through the "Necurs" botnet, with malicious attachments or links. Incorporation of new malware, creating custom malware, and the use of advanced tactics, such as the removal of malware artifacts, indicate that this group is a sophisticated threat and likely well-funded. The group is innovative and shows the flexibility to pivot to other techniques and malware trends on a global scale.[60]

TA505 conducts large-scale malspam campaigns that are distributed on a global level. The group has also been observed distributing malware in small, targeted campaigns with TA505 distributing custom malware like the group's "FlawedAmmyy" Remote Access Trojan (RAT), which was later used in more widespread campaigns.[61] The small-scale attacks typically target a financial institution with financially-themed malspam with the object of tricking email recipients into downloading malware (banking trojan, downloader, ransomware, RAT), typically by enabling malicious macros in an email attachment. The group's malspam has also been observed to attempt to trick recipients into following a malicious link (sometimes shortened) or downloading a malicious archive. The threat group will also use legitimately-signed certificates so the malware can impersonate legitimate software.[62]

Common TTPs

Malicious activity conducted by threat actors can vary across different types of groups. The different types of groups, for the purposes of this section, can be broken down into three categories: APT, Cybercriminal, and Hacktivist. The different motivations by threat actors in these categories will show some of the most common and different attack vectors and TTPs utilized by threat actors. The TTPs listed in subsequent sections is not a comprehensive list, threat actors utilize too many TTPs to do so, and some overlap amongst them is expected.

APT

APTs typically attempt to engage in long-term cyberespionage campaigns with the objective being information theft. That information can be owned by a variety of entities such as financial services, banking, education, government organizations, military, and technology, among others.

- Asymmetric Cryptography
- Boot or Logon Autostart Execution
- Boot or Logon Initialization Scripts
- Command and Scripting Interpreter
- Data Obfuscation
- Data Encoding
- Data Manipulation
- Exploit for Client Execution
- Exploitation for Credential Access
- Exploitation of Remote Services
- Hijack Execution Flow
- Indicator Removal on Host
- Obfuscate Files or Information
- Social Engineering
- Process Injection
- Scheduled Task
- Spearphishing Attachment
- Spearphishing Link
- Spearphishing via Service
- Supply Chain Compromise
- Symmetric Cryptography
- Template Injection
- User Execution

Cybercriminal

Cybercriminals are usually financially-motivated and will go to great lengths to accomplish their objectives, and in some instances their sophistication can rival state-sponsored APTs.

- Brute Force
- Data Encrypted for Impact
- Data Manipulation
- Defacement
- DLL Side-Loading
- Encrypted Channel
- Exploit for Client Execution
- Exploitation for Credential Access
- Exploitation of Remote Services
- Obfuscate Files or Information
- Phishing
- Process Injection
- Social Engineering
- Spearphishing Attachment
- Spearphishing Link
- Spearphishing via Service
- User Execution

Hacktivist

- Brute Force
- Data Encrypted for Impact
- Defacement
- Denial of Service (DoS)
- Distributed Denial of Service (DDoS)
- Phishing

Industry Targeting

The rise of accountability for cyberattacks set by standards posed by Global Data Protection Regulation (GDPR), in addition to massive data breaches such as Equifax in September 2017, have awakened the need to protect personally identifiable information (PII) handled by countless companies around the world. Nevertheless, there have been numerous cyber incidents affecting organizations in North America, with actors' primary objective being information theft.[63] Some of the most targeted industries in North America include:

1. Critical infrastructure / Energy
2. Entertainment / Media
3. Education
4. Financial services
5. Government
6. Manufacturing
7. Marketing
8. Medical
9. Retail / Hospitality
10. Technology
11. Transportation & Utilities

Threat actor activity, once they have gained access to a target, will vary depending on motive and sophistication, however, there are certain trends in this targeting that we have observed. For example, targeted ransomware attacks have increased around the globe, and the healthcare industry is especially vulnerable with the COVID-19 pandemic ongoing.[64]
In 2019, researchers found that small and medium-sized businesses were experiencing a "significant increase" in cyber incidents for a third consecutive year.[65] These global trends share similarities with malicious cyber activity affecting North America.

The most common types of malware families found targeting individuals and organizations in 2019 from most to least were: information stealers, cryptomining malware, and ransomware.[66] Some verticals experience more targeting of certain malware families, but may still be applicable to North America. In 2019 for example, education and retail were targeted mostly with Emotet, and that trojan remains one of the most widely-utilized malware families in the world as of this writing.[67] Other sectors, such as critical infrastructure, are targeted with more specialized malware instead of a commodity.

The critical infrastructure sector is targeted by numerous actors. Dragos researchers identified 11 different groups dedicated to attacking energy and critical infrastructure industries, seven of which targeted entities located in North America.[68] Based on the assessment that groups targeting infrastructure are not generally financially motivated, we judge that these groups are very likely already well-funded.. While information and destructive attacks typically affect these industries, global commodity campaigns have been observed impacting these industries as well due to the fact they have no discretion among targets. Groups that target critical infrastructure are usually incentivized by information, thus, these groups are also similar to those that target governments.

Sophisticated threat groups and APTs go through lengthy reconnaissance phases prior to launching operations on their true objective. These initial steps often include stealing user credentials to get access to other machines and systems on a target network.[69] Governments and associated organizations are at risk of being targeted by some of the most well-funded APT groups in the world, and these groups often develop and maintain their own custom malware in attempts to hide their activity.[70] Therefore, it is useful to maintain awareness of these groups to develop security practices to prevent this activity before it takes place. Furthermore, even amongst APTs, spearphishing remains a highly-used tactic that can be mitigated through education.

Conclusion

The North American cyber threat landscape is as complex as the region is vast. The largest economy in the world, the US, contributes greatly to cyber activity due to the numerous potential targets. However, there has been progress in protecting individuals' sensitive information that have been passed in multinational agreements, such as GDPR and USMCA. Countries who do not have robust economies have, or are beginning to, see the value in taking necessary steps to begin developing cyber and information security strategies and policies.

Endnotes

1 “1941: The Atlantic Charter,” United Nations, accessed September 15, 2020, https://www.un.org/en/sections/history-united-nations-charter/1941-atlantic-charter/index.html.

2 Bureau of Western Hemisphere Affairs, “U.S. Relations With Canada,” U.S. Department of State, accessed September 15, 2020, published July 16, 2020, https://www.state.gov/u-s-relations-with-canada/#:~:text=The%20United%20States%20and%20Canada%20enjoy%20the%20world’s%20most%20comprehensive,nearly%20%242%20billion%20per%20day.&text=Canada’s%20FDI%20stock%20in%20the%20United%20States%20totaled%20%24511%20billion.;%20https://www.nato.int/cps/en/natohq/nato_countries.htm.

3 “A Brief History of NORAD,” North American Aerospace Defense Command Office of History, accessed September 15, 2020, published December 31, 2013, https://www.norad.mil/Portals/29/Documents/A%20Brief%20History%20of%20NORAD%20(current%20as%20of%20March%202014).pdf, 4-5.

4 Alanna Petroff, et al., “These are America’s top trading partners,” CNN Money, accessed September 15, 2020, published December 2017, https://money.cnn.com/interactive/news/economy/how-us-trade-stacks-up/index.html#:~:text=China%2C%20Canada%20and%20Mexico%20are,and%20reworks%20free%20trade%20deals.;%20https://wits.worldbank.org/CountryProfile/en/Country/CAN/Year/2017/TradeFlow/EXPIMP/Partner/by-country#:~:text=In%202017%2C%20Canada%20major%20trading,%2C%20Mexico%2C%20Germany%20and%20Japan.

5 “Annual Merchandise Trade: Canada’s Merchandise Exports,” Global Affairs Canada, accessed September 15, 2020, published February 6, 2020, https://www.international.gc.ca/economist-economiste/statistics-statistiques/annual_merchandise_trade-commerce_des_marchandises_annuel.aspx?lang=eng.

6 “Border Crossing Entry Data | Annual Data,” U.S. Department of Transportation, accessed September 15, 2020, https://explore.dot.gov/views/BorderCrossingData/Annual?:isGuestRedirectFromVizportal=y&:embed=y.

7 Kurt Snibbe, “Here’s how much traffic crossed the U.S.-Mexico border,” The Mercury News, accessed September 15, 2020, published April 28, 2020, https://www.mercurynews.com/2019/04/05/heres-how-much-traffic-crosses-the-u-s-mexico-border/; “Border Crossing Entry Data | Annual Data,” U.S. Department of Transportation.

8 “Trade Statistics,” U.S. Customs and Border Protection, accessed September 15, 2020, published October 2, 2020, https://www.cbp.gov/newsroom/stats/trade.

9 Daniel Borunda, “DEA leader visits El Paso, talks cartels, COVID-19, Chapo and new most wanted drug lord,” El Paso Times, accessed September 15, 2020, published September 18, 2020, https://www.elpasotimes.com/story/news/crime/2020/09/17/dea-acting-chief-timothy-shea-talks-cartels-covid-19-el-paso/5793813002/; The Associated Press, “Death toll put at 20 for Mexico cartel attack near US border,” ABC News, accessed September 15, 2020, published December 2, 2019, https://abcnews.go.com/International/wireStory/toll-21-mexico-cartel-attack-us-border-67418347.

10 “Mexico rejects US intervention after Trump outlines drug cartel plan,” BBC, accessed September 15, 2020, published November 27, 2019, https://www.bbc.com/news/world-latin-america-50577522.

11 Martha C. White, “Trump sings USMCA trade deal to replace ‘nightmare NAFTA,’” NBC News, accessed September 16, 2020, published January 29, 2020, https://www.nbcnews.com/business/economy/trump-signs-usmca-trade-deal-replace-nightmare-nafta-n1125526; “President Donald J. Trump’s United States-Mexico-Canada Agreement Delivers a Historic Win for American Workers,” White House: Fact Sheets, accessed September 16, 2020, published January 29, 2020, https://www.whitehouse.gov/briefings-statements/president-donald-j-trumps-united-states-mexico-canada-agreement-delivers-historic-win-american-workers/.

12 “A new Canada-United States-Mexico Agreement,” Government of Canada, accessed September 16, 2020, published September 2, 2020, https://www.international.gc.ca/trade-commerce/trade-agreements-accords-commerciaux/agr-acc/cusma-aceum/index.aspx?lang=eng; “United States-Mexico-Canada Agreement,” Office of the United States Trade Representative, accessed September 17, 2020, https://ustr.gov/trade-agreements/free-trade-agreements/united-states-mexico-canada-agreement.

13 Thomas Franck, “US weighing 100% tariffs on more EU products including whiskies and Cognac, according to documents,” CNBC, accessed September 17, 2020, published December 15, 2019, https://www.cnbc.com/2019/12/13/ustr-weighing-100percent-tariffs-on-new-eu-products-including-whiskies.html.

14 Paul Hannon and Tom Fairless, “Trump’s Tariff Threats Are Tested by Europe’s Record Trade Surplus,” The Wall Street Journals, accessed September 17, 2020, published February 14, 2020, https://www.wsj.com/articles/trumps-tariff-threats-are-tested-by-europes-record-trade-surplus-11581682605.

15 “Joint Statement of the United States and the European Union on a Tariff Agreement,” Office of the United States Trade Representative, accessed September 17, 2020, published August 21, 2020, https://ustr.gov/about-us/policy-offices/press-office/press-releases/2020/august/joint-statement-united-states-and-european-union-tariff-agreement.

16 “Countries and regions: United States,” European Commission, accessed September 17, 2020, published April 23, 2020, https://ec.europa.eu/trade/policy/countries-and-regions/countries/united-states/.

17 David Lawder, “U.S. extends some China tariff exclusions only through year end,” Reuters, accessed September 15, 2020, published September 15, 2020, https://www.reuters.com/article/usa-trade-china-tariffs/u-s-extends-some-china-tariff-exclusions-only-through-year-end-idUSKBN25S5C5.

18 Ibid.; Federal Register, “Notice of Product Exclusion Extensions: China’s Acts, Policies, and Practices Related to Technology Transfer, Intellectual Property, and Innovation,” Office of the United States Trade Representative, accessed September

15, 2020, published September 2, 2020, https://www.federalregister.gov/documents/2020/09/02/2020-19419/notice-of-product-exclusion-extensions-chinas-acts-policies-and-practices-related-to-technology.

19 Kety Stech Ferek and Georgia Wells, “TikTok Download Ban Is Blocked by Judge,” The Wall Street Journal, accessed September 27, 2020, published September 27, 2020, https://www.wsj.com/articles/tiktok-makes-its-case-for-last-minute-reprieve-from-u-s-download-ban-11601225594.

20 Ibid.; Kari Paul, “Trump’s bid to ban TikTok and WeChat: where are we now,” accessed September 29, 2020, published September 29, 2020, https://www.theguardian.com/technology/2020/sep/29/trump-tiktok-wechat-china-us-explainer.

21 Alon Boxiner, et al., “Tik or Tok? Is TikTok secure enough,” Check Point Blog, accessed September 18, 2020, published January 8, 2020, https://research.checkpoint.com/2020/tik-or-tok-is-tiktok-secure-enough/.

22 Shivang Desai, “TikTok Spyware,” Zscaler Blog, accessed September 18, 2020, published September 8, 2020, https://www.zscaler.com/blogs/research/tiktok-spyware; Elizabeth Montalbano, “Spyware Labeled ‘TikTok Pro’ Exploits Fears of U.S. Ban,” Threatpost, accessed September 18, 2020, published September 9, 2020, https://threatpost.com/spyware-labeled-tiktok-pro-exploits-fears-of-us-ban/159050/.

23 Mari Meisenzahl, “Trump is considering banning Chinese social media app TikTok. See the full list of countries, companies, and organizations that have already banned it,” Business Insider, accessed September 21, 2020, published July 13, 2020, https://www.businessinsider.com/tiktok-banned-by-countries-organizations-companies-list-2020-7; Sara Fischer and Fadel Allassan, “TikTok faces bans around the world,” Axios, accessed September 21, 2020, published August 6, 2020, https://www.axios.com/tiktok-bans-worldwide-china-6e77a3a8-f4c7-4600-94bf-df89af0a8e5f.html.

24 Office of Public Affairs, “Chinese Telecommunications Conglomerate Huawei and Huawei CFO Wanzhou Meng Charged With Financial Fraud,” The United States Department of Justice, accessed September 21, 2020, published January 28, 2019, https://www.justice.gov/opa/pr/chinese-telecommunications-conglomerate-huawei-and-huawei-cfo-wanzhou-meng-charged-financial.

25 Moira Warburton and Tessa Vikander, “Canada lawyers asks judge to keep Huawei CFO’s U.S. extradition case ‘on the straight and narrow,’” Reuters, accessed September 21, 2020, published September 29, 2020, https://www.reuters.com/article/us-usa-huawei-tech-canada/huawei-lawyers-wrap-up-arguments-in-canadian-court-saying-us-extradition-case-is-ineffective-idUSKBN26K0Y3.

26 Wendy Wu, “No clear end to China-Canada relations slide which began with the arrest of Huawei’s Meng Wanzhou,” South China Morning Post, accessed September 21, published August 1, 2020, https://www.scmp.com/news/china/diplomacy/article/3095495/no-clear-end-china-canada-relations-slide-which-began-arrest.

27 “Canadian international merchandise trade, January 2020,” Statistics Canada, accessed September 21, 2020, published March 6, 2020, https://www150.statcan.gc.ca/n1/daily-quotidien/200306/dq200306b-eng.htm.

28 Eric Martin, “China and Mexico Lay Out Broad Plans to Strengthen Relations,” Bloomberg, accessed September 21, 2020, published July 2, 2019, https://www.bloomberg.com/news/articles/2019-07-02/china-and-mexico-lay-out-broad-plans-to-strengthen-relations.

29 “Mexican official eyes stronger ties with China after U.S. trade deal,” Reuters, accessed September 21, 2020, published January 19, 2020, https://www.reuters.com/article/us-mexico-china/mexican-official-eyes-stronger-ties-with-china-after-u-s-trade-deal-idUSKBN1ZI0PM.

30 “At least 10 companies from China seek to move to Mexico every month,” The Mazatlán Post, accessed September 21, 2020, published February 20, 2020, https://themazatlanpost.com/2020/02/20/at-least-10-companies-from-china-seek-to-move-to-mexico-every-month/.

31 “Xi says China ready to continue supporting Mexico in COVID-19 fight,” Xinhua, accessed September 21, 2020, published April 11, 2020, http://www.xinhuanet.com/english/2020-04/11/c_138965496.htm; Nayeli Lozano, “AMLO thanks Xi Jinping for support against coronavirus and sale and equipment,” Político MX, accessed September 21, 2020, published April 10, 2020, https://politico.mx/minuta-politica/minuta-politica-gobierno-federal/amlo-tendr%C3%A1-conferencia-telef%C3%B3nica-con-presidente-de-china-xi-jinping/.

32 Guatemala CERT, https://www.cyberseg.com/; Dominican Republic CERT, https://cncs.gob.do/csirt-rd/; Caribbean CERT, https://www.caricert.cw/; Mexico CERT, https://www.cert.org.mx/; Canada CERT, https://cyber.gc.ca/en/, US CERT, https://us-cert.cisa.gov/; Panama CERT, https://cert.pa/.

33 “NORTH AMERICA CYBER SECURITY MARKET – GROWTH, TRENDS, AND FORECASTS (2020 – 2025),” Mordor Intelligence, accessed September 22, 2020, https://www.mordorintelligence.com/industry-reports/north-america-cyber-security-market.

34 Logan Finucan, “USMCA: What’s in the Digital Chapter for Your Company,” Access Partnership, accessed September 22, 2020, published January 29, 2020, https://www.accesspartnership.com/usmca-whats-in-the-digital-chapter-for-your-company/#:~:text=USMCA%20is%20one%20of%20the,effective%20management%20of%20cyber%20risks.

35 Francoise Gilbert, “United States-Mexico-Canada Agreement: Digital Trade Provisions: NAFTA 2.0 meets the Internet,” Cloud Security Alliance, accessed September 22, 2020, published June 30, 2020, https://cloudsecurityalliance.org/blog/2020/06/30/united-states-mexico-canada-agreement-digital-trade-provisions-nafta-2-0-meets-the-internet/

36 Ibid.; “What is the Cross-Border Privacy Rules System?” Asia-Pacific Economic Cooperation, accessed September 22, 2020, published April 15, 2019, https://www.apec.org/About-Us/About-APEC/Fact-Sheets/What-is-the-Cross-Border-Privacy-Rules-System.

37 “Cybersecurity program,” Organization of American States, accessed September 22, 2020, http://www.oas.org/en/sms/cicte/

prog-cybersecurity.asp.

[38] Gage Mele, Parthiban R., and Tara Gould, “COVID-19 Themes Are Being Utilized by Threat Actors of Varying Sophistication,” Anomali Blog, accessed September 22, 2020, published March 23, 2020, https://www.anomali.com/blog/covid-19-themes-are-being-utilized-by-threat-actors-of-varying-sophistication; Tara Gould, Gage Mele, Parthiban Rajendran, and Rory Gould, “Anomali Threat Research Identifies Fake COVID-19 Contact Tracing Apps Used to Download Malware that Monitors Devices, Steals Personal Data,” Anomali Blog, accessed September 22, 2020, published June 10, 2020, https://www.anomali.com/blog/anomali-threat-research-identifies-fake-covid-19-contact-tracing-apps-used-to-monitor-devices-steal-personal-data; Sandra Joyce, “Limited Shifts in the Cyber Threat Landscape Driven by COVID-19,” FireEye Blog, accessed September 22, 2020, published April 8, 2020, https://www.fireeye.com/blog/threat-research/2020/04/limited-shifts-in-cyber-threat-landscape-driven-by-covid-19.html.

[39] Ibid.

[40] GReAT, “The MiniDuke Mystery: PDF 0-day Government Spy Assembler 0x29A Micro Backdoor,” Securelist, accessed September 25, published February 27, 2013, https://securelist.com/the-miniduke-mystery-pdf-0-day-government-spy-assembler-0x29a-micro-backdoor/31112/.

[41] “APT29,” MITRE | ATT&CK, accessed September 25, 2020, https://attack.mitre.org/groups/G0016/; “APT29,” ThreatStream, https://ui.threatstream.com/actor/12600.

[42] Ibid.

[43] Nalani Fraser, et al., “APT41 A Dule Espionage and Cyber Crime,” FireEye Blog, accessed September 25, published August 7, 2019, https://www.fireeye.com/blog/threat-research/2019/08/apt41-dual-espionage-and-cyber-crime-operation.html; Christopher Glyer, et al., “This Is Not a Test: APT41 Initiates Global Intrusion Campaign Using Multiple Exploits,” FireEye Blog, accessed September 25, 2020, published March 25, 2020, https://www.fireeye.com/blog/threat-research/2020/03/apt41-initiates-global-intrusion-campaign-using-multiple-exploits.html.

[44] Ibid.

[45] Ibid.

[46] Ibid.

[47] Ibid.

[48] Ibid.

[49] Ibid.

[50] Ibid.

[51] Ibid.

[52] “Charming Kitten,” MITRE | ATT&CK, https://attack.mitre.org/groups/G0058/.

[53] “Charming Kitten,” ClearSky Cyber Security, https://www.clearskysec.com/wp-content/uploads/2017/12/Charming_Kitten_2017.pdf, 53.

[54] Ibid., 47.

[55] “EQUATION GROUP: QUESTIONS AND ANSWERS,” Kaspersky, accessed September 27, 2020, published February 2015, https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2018/03/08064459/Equation_group_questions_and_answers.pdf, 3.

[56] Ibid., 4; “Gauss: Abnormal Distribution,” Kaspersky Lab, https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2018/03/20134940/kaspersky-lab-gauss.pdf, 3.

[57] “EQUATION GROUP: QUESTIONS AND ANSWERS,” Kaspersky, 27; “Gauss: Abnormal Distribution,” Kaspersky Lab, 10.

[58] “EQUATION GROUP: QUESTIONS AND ANSWERS,” Kaspersky, 15; “Gauss: Abnormal Distribution,” Kaspersky Lab, 4.

[59] “EQUATION GROUP: QUESTIONS AND ANSWERS,” Kaspersky, 8; “Gauss: Abnormal Distribution,” Kaspersky Lab, 38.

[60] “Threat Actor Profile: TA505, From Dridex to GlobeIImposter,” Proofpoint, accessed September 25, 2020, published September 27, 2017, https://www.proofpoint.com/us/threat-insight/post/threat-actor-profile-ta505-dridex-globeimposter; “TA505,” ThreatStream, https://ui.threatstream.com/actor/26092.

[61] Tom Spring, “TA505 Crooks are Now Targeting US Retailers with Personalized Campaigns,” Threatpost, accessed September 28, published December 7, 2018, https://threatpost.com/ta505-crooks-are-now-targeting-us-retailers-with-personalized-campaigns/139702/.

[62] Eli Salem, “THREAT ACTOR TA505 TARGETS FINANCIAL ENTERPRISES USING LOLBINS AND A NEW BACKDOOR MALWARE,” Cybereason Blog, accessed September 28, 2020, published April 25, 2019, https://www.cybereason.com/blog/threat-actor-ta505-targets-financial-enterprises-using-lolbins-and-a-new-backdoor-malware.

[63] Tara Seals, “Sharp Spike in Ransomware in the U.S. as Pandemic Inspires Attackers,” Threatpost, accessed September 28, 2020, published July 23, 2020, https://threatpost.com/sharp-spike-ransomware-pandemic-inspires-attackers/157689/

[64] Ibid.; Josh Fruhlinger, “Recent ransomware attacks define the malware’s new age,” CSO Online, accessed September 29, 2020, published February 20, 2020, https://www.csoonline.com/article/3212260/recent-ransomware-attacks-define-the-malwares-new-age.html.

[65] Charlie Osborne, “76 percent of US businesses have experienced a cyberattack in the past year,” ZDNet, accessed September

29, 2020, published October 8, 2019, https://www.zdnet.com/article/76-percent-of-us-businesses-have-experienced-a-cyberattack-in-the-past-year/.

66 Anjali Patil, et al., “Americas: How Managed Detection and Response Helps Address Persistent Threats,” Trend Micro, accessed September 29, 2020, Published March 7, 2019, https://www.trendmicro.com/vinfo/mx/security/news/cybercrime-and-digital-threats/threat-landscape-in-the-americas-how-managed-detection-and-response-helps-address-persistent-threats.

67 “2020 State of Malware Report,” Malwarebytes Labs, accessed September 29, 2020, published February 2020, https://resources.malwarebytes.com/files/2020/02/2020_State-of-Malware-Report-1.pdf, 49-50.

68 “North American Electric Cyber Threat Perspective,” Dragos, accessed September 29, 2020, published January 2020, https://www.dragos.com/wp-content/uploads/NA-EL-Threat-Perspective-2019.pdf, 2-6.

69 Anomali Threat Research, “Phishing Campaign Targets Login Credentials of Multiple US, International Government Procurement Services,” Anomali Blog, accessed September 29, 2020, published December 12, 2019, https://www.anomali.com/blog/phishing-campaign-targets-login-credentials-of-multiple-us-international-government-procurement-services.

70 Sara Moore, Joakim Kennedy, Parthiban R., and Rory Gould, “Anomali Suspects that China-Backed APT May Be Seeking Access to Vietnam Government Data Center,” Anomali Blog, accessed September 29, 2020, published April 30, 2020, https://www.anomali.com/blog/anomali-suspects-that-china-backed-apt-pirate-panda-may-be-seeking-access-to-vietnam-government-data-center; Gage Mele and Parthiban R., “Malicious Activity Aligning with Gamaredon TTPs Targets Ukraine,” Anomali Blog, accessed September 29, 2020, published December 5, 2019, https://www.anomali.com/blog/malicious-activity-aligning-with-gamaredon-ttps-targets-ukraine; “Palmerworm: Espionage Gang Targets the Media, Finance, and Other Sectors,” Symantec Blog, accessed September 29, 2020, published September 29, 2020, https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/palmerworm-blacktech-espionage-apt.

71 “Threat Group Cards: A Threat Actor Encyclopedia,” ThaiCERT, accessed September 10, 2020, published July 2020, https://www.dropbox.com/s/ds0ra0c8odwsv3m/Threat%20Group%20Cards.pdf?dl=0, 375; “”Achilles”, Hacker Behind Attacks on Military Shipbuilders, UNICEF & International Corporations,” Advanced Intel, accessed September 10, 2020, published September 4, 2019, https://www.advanced-intel.com/post/achilles-hacker-behind-attacks-on-military-shipbuilders-unicef-international-corporations; Ionut Ilascu, “Another Hacker Selling Access to Charity, Antivirus Firm Networks,” BleepingComputer, accessed September 10, 2020, published June 6, 2019, https://www.bleepingcomputer.com/news/security/another-hacker-selling-access-to-charity-antivirus-firm-networks/.

72 Robert Falcone and Brittany Barbehenn, “Aggah Campaign, Bit.ly, BlogSpot, and Pastebin Used for C2 in Large Scale Campaign,” Palo Alto Networks, accessed September 10, 2020, published April 17, 2019, https://unit42.paloaltonetworks.com/aggah-campaign-bit-ly-blogspot-and-pastebin-used-for-c2-in-large-scale-campaign/.

73 “ALLANITE,” Dragos, accessed September 10, 2020, https://www.dragos.com/threat/allanite/.

74 Adam Meyers, “Who is Anchor Panda,” Crowdstrike Blog, accessed September 10, 2020, published March 23, 2013, https://www.crowdstrike.com/blog/whois-anchor-panda/.

75 “Deputy Dog,” ThreatStream, https://ui.threatstream.com/actor/26897.

76 “APT28,” ThreatStream, https://ui.threatstream.com/actor/4494.

77 “APT29,” ThreatStream, https://ui.threatstream.com/actor/12600.

78 “Bamboo Spider,” ThreatStream, https://ui.threatstream.com/actor/27832.

79 “Bronze Butler,” ThreatStream, https://ui.threatstream.com/actor/3722.

80 “Carbanak,” ThreatStream, https://ui.threatstream.com/actor/1688.

81 “Charming Kitten,” ThreatStream, https://ui.threatstream.com/actor/5115.

82 “How the Nasty Netwalker Behaved in the Past Few Months,” Cyware, accessed September 11, 2020, published August 26, 2020,

83 Michael Gorelik, “COBALT GROUP 2.0,” Morphisec Blog, accessed Sept 11, 2020, published October 8, 2018, https://blog.morphisec.com/cobalt-gang-2.0; “Threat Group Cards: A Threat Actor Encyclopedia,” ThaiCERT, 85.

84 “Deep Panda,” ThreatStream, https://ui.threatstream.com/actor/1724.

85 GReAT, “THE DESERT FALCONS TARGETED ATTACKS,” Kaspersky Lab, https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2018/03/08064309/The-Desert-Falcons-targeted-attacks.pdf, 4.

86 “Elderwood,” ThreatStream, https://ui.threatstream.com/actor/14721.

87 “Threat Group-3390,” MITRE | ATT&CK, https://attack.mitre.org/groups/G0027/.

88 “EQUATION GROUP: QUESTIONS AND ANSWERS,” Kaspersky, 3.

89 “FIN4,” ThreatStream, https://ui.threatstream.com/actor/26694.

90 “FIN5,” ThreatStream, https://ui.threatstream.com/actor/14711.

91 Michael Gorelik and Alon Groisman, “NEW GLOBAL CYBER ATTACK ON POINT OF SALE SYSTEMS,” Morphisec Blog, accessed September 15, 2020, published February 27, 2019, https://blog.morphisec.com/new-global-attack-on-point-of-sale-systems; Brendan McKeague, et al., “Pick-Six: Intercepting a FIN6 Intrusion, an Actor Recently Tied to Ryuk and LockerGoga Ransomware,” FireEye Blog, accessed September 15, 2020, published April 5, 2019, https://www.fireeye.com/blog/threat-research/2019/04/pick-six-intercepting-a-fin6-intrusion.html.

92 “FIN7,” ThreatStream, https://ui.threatstream.com/actor/1731.

[93] “FIN8,” ThreatStream, https://ui.threatstream.com/actor/14714.

[94] “FIN10,” ThreatStream, https://ui.threatstream.com/actor/14710.

[95] “Threat Group Cards: A Threat Actor Encyclopedia,” ThaiCERT, 138; Matt Dahl, “Cat Scratch Fever: Crowdstrike Tracks Newly Reported Iranian Actor as FLYING KITTEN,” Crowdstrike Blog, accessed September 15, 2020, published May 13, 2014, https://www.crowdstrike.com/blog/cat-scratch-fever-crowdstrike-tracks-newly-reported-iranian-actor-flying-kitten/.

[96] FortiGuard SE Team, “CTA Adversary Playbook: Goblin Panda,” Fortinet Blog, accessed September 15, 2020, published November 1, 2018, https://www.fortinet.com/blog/threat-research/cta-security-playbook--goblin-panda.

[97] “Gorgon Group,” MITRE | ATT&CK, https://attack.mitre.org/groups/G0078/.

[98] “Threat Group Cards: A Threat Actor Encyclopedia,” ThaiCERT, accessed September 14, 2020, https://www.thaicert.or.th/downloads/files/A_Threat_Actor_Encyclopedia.pdf, 113.

[99] Alexander Hanel, “Big Game Hunting with Ryuk: Another Lucrative Targeted Ransomware,” Crowdstrike Blog, accessed September 14, 2020, published January 10, 2019, https://www.crowdstrike.com/blog/big-game-hunting-with-ryuk-another-lucrative-targeted-ransomware/.

[100] A L Johnson, “Hidden Lynx – Professional Hackers for Hire,” Broadcom Blog, accessed September 14, 2020, published September 17, 2013, https://community.broadcom.com/symantecenterprise/communities/community-home/librarydocuments/viewdocument?DocumentKey=8962de07-8e6a-41cc-a6d6-d22ea52dcbfa&CommunityKey=1ecf5f55-9545-44d6-b0f4-4e4a7f5f5e68&tab=librarydocuments.

[101] “HE ‘ICEFOG’ APT: A TALE OF CLOAK AND THREE DAGGERS,” Kaspersky Lab, accessed September 14, 2020, published September 2013, https://media.kaspersky.com/en/icefog-apt-threat.pdf, 3; Pierluigi Paganini, “Hunting the ICEFOG APT group after years of silence,” Security Affairs, accessed September 14, 2020, published June 8, 2019, https://securityaffairs.co/wordpress/86826/apt/icefog-apt-group-return.html.

[102] “Infy,” Malpedia, https://malpedia.caad.fkie.fraunhofer.de/actor/infy; Tomer Bar, et al., “Prince of Persia – Game Over,” Palo Alto Networks, accessed September 14, 2020, published June 28, 2016, https://unit42.paloaltonetworks.com/unit42-prince-of-persia-game-over/.

[103] “Lazarus Group,” ThreatStream, https://ui.threatstream.com/actor/281.

[104] Microsoft Defender ATP Research Team, “Detecting threat actors in recent German industrial attacks with Windows Defender ATP,” Microsoft Security Blog, accessed September 14, 2020, published January 25, 2017, https://www.microsoft.com/security/blog/2017/01/25/detecting-threat-actors-in-recent-german-industrial-attacks-with-windows-defender-atp/.

[105] “Threat Group Cards: A Threat Actor Encyclopedia,” ThaiCERT, https://www.thaicert.or.th/downloads/files/A_Threat_Actor_Encyclopedia.pdf, 138; “Leafminer,” MITRE | ATT&CK, https://attack.mitre.org/groups/G0077/.

[106] “Leviathan,” ThreatStream, https://ui.threatstream.com/actor/12582.

[107] “Threat Group Cards: A Threat Actor Encyclopedia,” ThaiCERT, https://www.thaicert.or.th/downloads/files/A_Threat_Actor_Encyclopedia.pdf, 162.

[108] “Lunar Spider,” ThreatStream, https://ui.threatstream.com/actor/27023.

[109] “Threat Group Cards: A Threat Actor Encyclopedia,” ThaiCERT, https://www.thaicert.or.th/downloads/files/A_Threat_Actor_Encyclopedia.pdf, 147.

[110] “MageCart,” ThreatStream, https://ui.threatstream.com/actor/21764.

[111] “Cobalt Gypsy,” ThreatStream, https://ui.threatstream.com/actor/1903.

[112] “Threat Group Cards: A Threat Actor Encyclopedia,” ThaiCERT, https://www.thaicert.or.th/downloads/files/A_Threat_Actor_Encyclopedia.pdf, 151.

[113] Yonathan Klijnsma, et al., “Mofang A politically motivated information stealing adversary,” Fox-IT, accessed September 15, 2020, published May 17, 2016, https://foxitsecurity.files.wordpress.com/2016/06/fox-it_mofang_threatreport_tlp-white.pdf, 1.

[114] “Threat Group Cards: A Threat Actor Encyclopedia,” ThaiCERT, https://www.thaicert.or.th/downloads/files/A_Threat_Actor_Encyclopedia.pdf, 153.

[115] “MoneyTaker,” ThreatStream, https://ui.threatstream.com/actor/26316.

[116] “Mummy Spider,” ThreatStream, https://ui.threatstream.com/actor/27288.

[117] “Threat Group Cards: A Threat Actor Encyclopedia,” ThaiCERT, https://www.thaicert.or.th/downloads/files/A_Threat_Actor_Encyclopedia.pdf, 165.

[118] Ibid., 166.

[119] Ibid., 168.

[120] “OilRig,” ThreatStream, https://ui.threatstream.com/actor/4411.

[121] “Orangeworm,” ThreatStream, https://ui.threatstream.com/actor/12577.

[122] “Palmerworm: Espionage Gang Targets the Media, Finance, and Other Sectors,” Symantec Blog.

[123] The BlackBerry Research and Intelligence Team, “Decade of RATs: Novel APT Attacks Targeting Linux, Windows and Android,” BlackBerry Blog, accessed September 15, 2020, published April 7, 2020, https://blogs.blackberry.com/

en/2020/04/decade-of-the-rats.

124 “Patchwork,” ThreatStream, https://ui.threatstream.com/actor/14704.

125 “Pinchy Spider,” ThreatStream, https://ui.threatstream.com/actor/27936.

126 “Threat Group Cards: A Threat Actor Encyclopedia,” ThaiCERT, https://www.thaicert.or.th/downloads/files/A_Threat_Actor_Encyclopedia.pdf, 187.

127 Crowdstrike Global Intelligence Team, “Putter Panda,” Crowdstrike, accessed September September 16, published May 2, 2014, http://cdn0.vox-cdn.com/assets/4589853/crowdstrike-intelligence-report-putter-panda.original.pdf, 4-5.

128 “Threat Group Cards: A Threat Actor Encyclopedia,” ThaiCERT, https://www.thaicert.or.th/downloads/files/A_Threat_Actor_Encyclopedia.pdf, 197.

129 “DNS Infrastructure Hijacking Campaign,” Cybersecurity & Infrastructures Security Agency, accessed September 16, 2020, published February 13, 2019, https://us-cert.cisa.gov/ncas/alerts/AA19-024A; Danny Adamitis, et al., “DNS Hijacking Abuses Trust in Core Internet Service,” Cisco Talos Blog, accessed September 16, 2020, published April 18, 2020, https://blog.talosintelligence.com/2019/04/seaturtle.html.

130 “Silence,” ThreatStream, https://ui.threatstream.com/actor/26796.

131 “Silent Librarian,” ThreatStream, https://ui.threatstream.com/actor/11439.

132 “Animal Farm APT and the Shadow of French Intelligence,” Infosec Institute, accessed September 17, 2020, published August 8, 2015, https://resources.infosecinstitute.com/animal-farm-apt-and-the-shadow-of-france-intelligence/.

133 “APT10,” ThreatStream, https://ui.threatstream.com/actor/1174.

134 “Threat Group Cards: A Threat Actor Encyclopedia,” ThaiCERT, https://www.dropbox.com/s/ds0ra0c8odwsv3m/Threat%20Group%20Cards.pdf?dl=0, 313.

135 Edmund Brumaghin, et al., “SWEED: Exposing years of Agent Tesla campaigns,” Cisco Talos Blog, accessed September 17, 2020, published July 15, 2019, https://blog.talosintelligence.com/2019/07/sweed-agent-tesla.html.

136 “Threat Group Cards: A Threat Actor Encyclopedia,” ThaiCERT, https://www.dropbox.com/s/ds0ra0c8odwsv3m/Threat%20Group%20Cards.pdf?dl=0, 317.

137 “TA505,” ThreatStream, https://ui.threatstream.com/actor/26092.

138 “TA544,” ThreatStream, https://ui.threatstream.com/actor/27912.

139 “DanaBot – A new banking Trojan surfaces Down Under,” Proofpoint Blog, accessed September 18, 2020, published May 31, 2018, https://www.proofpoint.com/us/threat-insight/post/danabot-new-banking-trojan-surfaces-down-under-0.

140 Bryan Campbell, et al., “TA2101 plays government imposter to distribute malware to German, Italian, and US organizations,” Proofpoint Blog, accessed September 18, 2020, published November 14, 2019, https://www.proofpoint.com/us/threat-insight/post/ta2101-plays-government-imposter-distribute-malware-german-italian-and-us; Jeremy Kennelly, et al., “Navigating MAZE: Tactics, techniques and Procedures Associated With MAZE Ransomware Incidents,” FireEye Blog, accessed September 18, 2020, published May 7, 2020, https://www.fireeye.com/blog/threat-research/2020/05/tactics-techniques-procedures-associated-with-maze-ransomware-incidents.html.

141 Chris Brook, “Data Stealing Malware TeamSpy Resurfaces in Spam Campaign,” Threatpost, accessed September 18, 2020, published February 21, 2017, https://threatpost.com/data-stealing-malware-teamspy-resurfaces-in-spam-campaign/123820/; Dennis Fisher, “Researchers Uncover ‘TeamSpy’ Attack Campaign Against Government, Research Targets,” Threatpost, accessed September 18, 2020, published March 20, 2013, https://threatpost.com/researchers-uncover-teamspy-attack-campaign-targeting-government-research-targets-032013/77646/.

142 “admin@338,” ThreatStream, https://ui.threatstream.com/actor/2033.

143 “Thrip,” ThreatStream, https://ui.threatstream.com/actor/61241.

144 “2019 Global Threat Report,” Crowdstrike, https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2019GlobalThreatReport.pdf, 55.

145 “Turla,” ThreatStream, https://ui.threatstream.com/actor/1145.

146 “Threat Group Cards: A Threat Actor Encyclopedia,” ThaiCERT, https://www.dropbox.com/s/ds0ra0c8odwsv3m/Threat%20Group%20Cards.pdf?dl=0, 359.

147 “Wizard Spider,” ThreatStream, https://ui.threatstream.com/actor/27829.

148 “Threat Group Cards: A Threat Actor Encyclopedia,” ThaiCERT, https://www.dropbox.com/s/ds0ra0c8odwsv3m/Threat%20Group%20Cards.pdf?dl=0, 364.

149 “Winnti,” ThreatStream, https://ui.threatstream.com/actor/827.

150 “Wizard Spider,” ThreatStream, https://ui.threatstream.com/actor/27829.

Appendix A

Table 1. Threat Groups that Target North America

Threat Actor/Group	Description	Country of Origin
Achilles	English speaking and financially-motivated group. Achilles objective consists of gaining access to high-value corporate networks.[71] Possibly associated with the Iridium group.	Unknown
Aggah	Information-motivated group that uses commodity malware primarily delivered through malicious documents.[72]	Unknown
Allanite	Cyberespionage group that primarily targets industrial control networks of companies in the energy sector.[73]	Unknown
Anchor Panda (APT14, Aluminum)	Targets countries with interest in the South China Sea in addition to western companies in multiple industries.[74]	China
APT17 (Deputy Dog)	Cyberespionage group that targets entities with BLACKCOFFEE malware which is able to disguise malicious traffic.[75]	China
APT28 (Fancy Bear, Group 74, Pawn Storm, Sofacy, Sednit, SnakeMackerel, Swallowtail, Strontium, Tsar Team)	The group is believed to operate under the Main Intelligence Directorate (GRU), and has been active since at least 2007. Known for compromising USA's Democratic National Committee in 2015.[76]	Russia
APT29 (Cozy Bear, Cozy Duke, Mini Duke, The Dukes)	The group boasts an arsenal of custom and complex malwares at its disposal and is believed to be sponsored by the Russian Federation government. APT29 is known for compromising USA's Democratic National Committee in 2016, and has been active since at least 2008.[77]	Russia
Bamboo Spider (Panda Zeus, Panda Banker, Zeus Panda)	Financially-motivated group known for creating the Panda Banker (PandaBot, Zeus Panda) commodity banking trojan.[78]	Unknown
Bronze Butler (Stalker Panda, Tick, REDBALDKNIGHT)	The group's objective is to steal information while attempting to maintain a presence in compromised environments. Bronze Butler uses both proprietary and publicly available tools to conduct their malicious activity.[79]	China
Carbanak (Anunak, Carbon Spider)	Financially-motivated group that has been active since at least 2013. They are a sophisticated group that will compromise vendors employed by the primary target to use the vendor's legitimate emails in spearphishing campaigns.[80]	Ukraine

Threat Actor/Group	Description	Country of Origin
Charming Kitten (iKittens, NewsBeef, Newscasters)	Cyberespionage group that conducts widespread campaigns on numerous entities in multiple sectors.[81]	Iran
Circus Spider	Cybercriminal group that develops and operates the NetWalker ransomware.[82]	Unknown
Cobalt Group (Cobalt Spider, Cobalt Gang, Gold Kingswood)	Financially-motivated threat groups that has attacked entities in multiple sectors with a variety of malware and tools.[83]	Russia
Deep Panda (APT26, Shell Crew, WebMasters, KungFu Kittens, Group 13, PinkPanther, Black Vine)	Cyberespionage group that conducts campaigns that primarily target the USA, however multiple other countries are also targeted. This includes an interest in countries and entities associated to, and located in, the Asia Pacific region.[84]	China
Desert Falcons (APT-C-23, Two-tailed Scorpion)	Information-motivated group that consists of approximately 30 members around the world that spend the time necessary to create convincing fake material for their campaigns.[85]	Gaza
Elderwood (Elderwood Gang, Sneaky Panda, SIG22, Beijing Group)	Motivated by the theft of proprietary information and was first identified in 2012. Believed to consist of different sub-groups each with their own specific targeting. Elderwood uses a platform, that contains various exploits utilized in spearphishing and watering-hole campaigns.[86]	China
Emissary Panda (APT27, LuckyMouse, Bronze Union, TG-3390, TEMP.Hippo, Group 35)	Utilizes strategic web compromise to target organizations with the objective of information theft.[87]	China
Equation Group	The group is highly sophisticated and is believed to have been active since at least 2001. Equation primarily targets entities located in the Middle East with custom and complex malware.[88]	US
FIN4 (Wolf Spider)	Financially-motivated threat group that has targeted email accounts of individuals believed to be in possession of sensitive information, often in the form of financial documents such as stock trading.[89]	Romania
FIN5	Financially-motivated group that primarily uses compromised credentials as their initial infection vector.[90]	Unknown
FIN6 (Skeleton Spider)	Financially-motivated group known for targeting point of sale (PoS) systems around the world.[91]	Unknown
FIN7	Sophisticated group that targets numerous sectors primarily located in Europe and the US.[92]	Russia

Threat Actor/Group	Description	Country of Origin
FIN8	Financially-motivated group that primarily targets the retail and hospitality industries in North America.[93]	Unknown
FIN10	Financially-motivated threat group active since at least 2013 through 2016 that targeted different organizations in North America with a particular focus on Canada.[94]	Unknown
Flying Kitten (Ajax Security Team, Group 26)	Transitioned from a web-defacements group to cyberespionage operations.[95]	Iran
Goblin Panda (Cycldek)	Data-motivated group that appears to target any country with interest in the South China Sea.[96]	China
Gorgon Group (Subaat)	Conducts a combination of criminal and specifically-targeted attacks.[97]	Pakistan
GozNym	Financially-motivated group that created GozNym trojan based on Nymain and Gozi (IFSB, Ursnif).[98]	Unknown, Multiple
Grim Spider	Sub group of Wizard Spider that operates targeted Ryuk ransomware campaigns.[99]	Russia
Hidden Lynx (Aurora Panda, Group 8)	Cyberespionage group that offers "professional hackers for hire."[100]	China
Icefog (Dagger Panda)	APT group that targets numerous industries, often in supply chain attacks, and uses multiple tools to steal sensitive data.[101]	China, Japan, South Korea
Infy (Prince of Persia, Operation Mermaid)	Cyberespionage group that target English and Persian-speaking individuals associated with civil and human rights activists.[102]	Middle East, likely Iran
Lazarus Group (Hidden Cobra, Guardians of Peace, Dark Seoul, New Romanic Cyber Army, Whois Hacking team)	APT group is well known for their tendency to engage in data destruction/disk wiping attacks, and DDoS attacks against targets around the world. Operatives are believed to be distributed throughout strategical geographic locations.[103]	North Korea
Lead	Associated with groups that use the Winnti malware that focuses on industrial espionage.[104]	China
Leafminer (Raspite)	Cyberespionage group that primary targets entities in the Middle East with the exception of the US.[105]	Iran
Leviathan (APT40, TEMP. Periscope, TEMP.Jumper, Bronze Mohawk, Mudcarp)	Leviathan conducts cyber espionage operations primarily on maritime, naval defense contractors, and associated research targets across multiple industries. The group's targets are primarily located in the United States and Western Europe.[106]	China

Threat Actor/Group	Description	Country of Origin
Lotus Panda (Naikon, Hellsing)	Group that focuses on countries located in, and with interest in, the South China Sea.[107]	China
Lunar Spider (BokBot)	Financially-motivated threat group known for creating the BokBot malware.[108]	Russia
Madi (Mahdi)	Cyberespionage group that targets entities around the world.[109]	Iran
Magecart	The umbrella term, MageCart, refers to groups that target online commercial websites and injects payment skimming scripts to illicitly obtain credit card credentials.[110]	Unknown
Magic Hound (APT35, Cobalt Gypsy, Rocket Kitten, TEMP.Beanie, Timberworm, Tarh Andishan)	Cyberespionage group that focuses on long-term information-theft campaigns. Group is believed to be an evolution of the Covellite threat group.[111]	Iran
Moafee	Cyberespionage group that focuses on countries with interest in the South China Sea.[112]	China
Mofang	Cyberespionage group that began operation targeting entities located in Myanmar (Burma), and now targets on a wider scale.[113]	China
Molerats (Extreme Jackal, Gaza Cybergang, Gaza Hackers Team)	Cybercriminal and politically-motivated group.[114]	Gaza
MoneyTaker	Financially-motivated group that has targeted companies around the world, and either attempts to make fraudulent money transfers or compromise card processing systems to steal data. Both open source and custom-created tools are utilized by MoneyTaker to conduct their malicious activity.[115]	Russia
Mummy Spider (TA542, Emotet, Mealybug, Geodo)	Financially-motivated group that operates the Emotet botnet.[116]	Unknown
NetTraveler (APT21)	Cyberespionage group that targets high profile individuals to install surveillance malware on their machines.[117]	China

Threat Actor/Group	Description	Country of Origin
Night Dragon	Cyberespionage group that targeted high profile individuals and companies in various industries by first locating and exploiting vulnerabilities.[118]	China
Nitro (Covert Grove)	Cyberespionage group that has grown through the years to incorporate targeting of multiple industries around the world.[119]	China
OilRig (APT34, Helix Kitten, Twisted Kitten, Crambus, Chrysene)	OilRig conducts cyberespionage operations focused on reconnaissance that benefits Iranian nation-state interests.[120]	Iran
Orangeworm	Orangeworm conducts corporate espionage operations, primarily on healthcare entities, but also on secondary targets that serve the healthcare industry. Other main targets include software, energy and engineering organizations.[121]	Unknown
Palmerworm	Cyberespionage group that utilizes custom malware to target multiple sectors in various countries around the world.[122]	Unknown
PassCV	Group utilizes publicly-available malware and tools and stolen.[123]	China
Patchwork (Dropping Elephant, Chinastrats, APT-C-09, Monsoon, Quilted Tiger)	Cyberespionage group that primarily targets diplomatic agencies, government entities, and think tanks. Patchwork's TTPs were originally tracked as individual campaigns called Operation Hangover (began in 2013) and Operation Monsoon (began in 2015).[124]	India
Pinchy Spider (Gold Southfield, Gold Garden)	Ransomware-as-a-service group that operates GandCrab, and later Sodinokibi (REvil).[125]	Russia
Poseidon Group	Portuguese-speaking threat group that engages in long-term cyberespionage campaign for the purpose of data theft.[126]	Unknown
Putter Panda (APT2, TG-6952, Group 36, Sulphur)	Cyberespionage group focused on Defense, Government, and Research sectors in the US.[127]	China
Samurai Panda (APT4, Wisp Team)	Cyberespionage group that primarily uses spearphishing emails targeting Asian democratic countries.[128]	China

Threat Actor/Group	Description	Country of Origin
Sea Turtle	Cyberespionage group that primary uses DNS hijacking as their initial infection vector.[129]	Unknown
Silence (Contract Crew, Whisper Spider, TEMP. TruthTeller, ATK 86)	Financially-motivated group-for-hire that is suspected to be made up of cybersecurity professionals who have migrated towards conducting black hat activities.[130]	Unknown
Silent Librarian (Mabna Institute)	Cyberespionage group on stealing academic and research materials to energy, medical, technical fields.[131]	Iran
Snowglobe (Animal Farm)	Creates custom spyware designed to conduct cyberespionage objectives.[132]	France
Stone Panda (APT10, menuPass, menuPass Team, Red Apollo, CVNX, Potassium, Hogfish, Happyyongzi)	Gained notoriety by targeting defense contractors around the world, but primarily those located in the U.S.[133, 124]	China
Strider (ProjectSauron)	Has targeted companies and individuals in cyberespionage campaigns since 2011.[134]	US
Sweed	Cyberespionage group that uses commodity malware to gain and maintain access while stealing information.[135]	Unknown
Syrian Electronic Army (SEA, Deadeye Jackal, ATK 196, TAG-CT2, Syria Malware Team)	Conducts information-theft and cyberespionage in apparent support of Syrian President Bashar al-Assad.[136]	Syria
TA505 (Graceful Spider, Gold Evergreen, TEMP. Warlock, Hive0065, Chimborazo)	Financially-motivated threat group that distributes commodity and customer malware.[137]	Unknown
TA544 (Cutwail V2, Narwhal Spider)	Financially-motivated group and the criminal operator of the Cutwail botnet version 2 (Cutwail V2).[138]	Unknown
TA547 (Scully Spider)	Financially-motivated threat group known for using commodity malware, such as DanaBot.[139]	Unknown

Threat Actor/Group	Description	Country of Origin
TA2101	Financially-motivated threat group that conducts specific spearphishing, and social engineering overall, campaigns with different commodity malware.[140]	Unknown
TeamSpy Crew (SIG39, Iron Lyric)	Known for conducting long-term cyberespionage campaigns that incorporates the legitimate use of TeamViewer app, as well as other commodity and authentic tools, in their malicious activity.[141]	Russia
Temper Panda (admin@338, Team338, Magnesium)	Conducts cyberespionage campaigns on targets in the defense sectors, financial services, government, and telecommunications industry.[142]	China
Thrip	Cyberespionage group that primarily targets entities in communications and telecommunications as well as defense contractors.[143]	China
Tiny Spider	Financially-motivated group behind the TinyLoader and TinyPOS malware.[144]	Unknown
Turla (Waterbug, Venomous Bear, Group 88, SIG23, Iron Hunter, Pacifier APT)	Connected to the "Epic" cyber espionage campaign that targets government agencies around the globe, and is also connected to the Agent.btz worm that infected the network of the U.S. Department of Justice in 2008.[145]	Russia
Volatile Cedar (Dancing Syndrome)	Targets companies and institutions with custom malware for the objective of information theft.[146]	Lebanon
Wicked Spider (APT22)	Wicked Spider is suspected to be a Chinese adversary-for-hire and is believed to be part of the larger "Winnti" group. The Spider cryptonym is used to represent the financially motivated activity of Winnti, whilst Panda is used to represent the intrusion activity.[147]	China
Wild Neutron (Butterfly, Sphinx Moth, Morpho, The Postal Group)	Financially-motivated group known for targeting high-profile companies in the early months of 2013.[148]	Unknown

Threat Actor/Group	Description	Country of Origin
Winnti Group (Blackfly, Wicked Panda)	Known for frequently targeting the gaming industry before expanding to other cybercrime activity. Winnti has been active since at least 2010 and has consistently updated their TTPs over the past decade.[149]	China
Wizard Spider (TheTrick, TrickBot)	Financially-motivated group that operates targeting campaigns using Ryuk ransomware and develops the Trickbot botnet.[150]	Russia