Under the Lens

The Asset and Wealth Management Sector

Cyber Threat Operations

Q2 2020

pwc

Contents

Introduction

The Asset and Wealth Management (AWM) sector plays a vital role in managing the world's financial capital, dealing in significant transactions across many industries. It is estimated that by 2025 the AWM sector will be worth approximately USD 145 trillion globally.[1] With such large amounts of wealth being handled by the sector, it garners much attention from threat actors of all motivations, particularly those seeking financial gain.

Over recent years, many financial institutions and regulators have noted the substantial surge in attacks on the financial sector as a whole - 2018 saw a 500% increase in data breaches across the wider financial sector over the preceding year according to the UK's Financial Conduct Authority (FCA).[2] The significant funds managed by the AWM sector are likely to attract threat actors seeking direct monetary gain, where high-value fraud attempts via business email compromise (BEC) and ransomware attacks remain popular attack vectors.

The sector is becoming increasingly competitive, with rising costs and new players in the market putting pressure on individual organisations to survive. As one of the more mature sectors in terms of technological innovations, many state-of-the-art technologies developed by successful organisations, including "Fintech", large scale data modelling, and new technologies surrounding virtual currencies, are potentially of great interest to those in a competitive scenario. Furthermore, the theft of specialised data, such as investment algorithms and models could seriously undermine business operations for those in the sector.

The COVID-19 pandemic has heavily reduced the operational capability of all sectors. In stark contrast, PwC has observed cyber activity rise, with threat actors leveraging this period of disruption for their own gain. As many organisations within the AWM sector have adapted to virtual working environments, there is a need to be more vigilant than ever when it comes to cyber security awareness. With so much capital at stake, in a sector that is guided fundamentally by risk appetite, it is vital that organisations within the sector maintain and uphold a robust, secure environment, as well as have the capability to detect and respond to attacks such that the business impact, if any, is minimised.

This report provides an overview of the most common cyber threats facing the AWM sector in order to generate awareness and illustrate the motivations behind such attacks, as well as support intelligence-led defence.

Our analysis is informed by our own in-house intelligence datasets maintained on cyber attacks and targeting from a variety of threat actors, intelligence gleaned from our incident response engagements around the world, as well as publicly-available reports on attacks in the sector.

[1] PwC, 'Asset & Wealth Management Revolution', https://www.pwc.com/gx/en/industries/financial-services/asset-management/publications/asset-wealth-management-revolution.html

[2] 'Cyber attacks on financial services sector rise fivefold in 2018', Financial Times, https://www.ft.com/content/6a2d9d76-3692-11e9-bd3a-8b2a211d90d5 (24th February 2019)

COVID-19 impact

The consequences of the COVID-19 situation have hit all sectors to varying degrees, with the AWM sector being no exception. Alongside the economic downturn, organisations face a juxtaposing increase in activity from threat actors of all motivations.

Whether it be espionage actors operating on behalf of interested parties with economic interests at play in a time of turmoil, or organised crime groups looking for new sources of income with consumer spending being down, illicit cyber activity is on the rise.

In particular, PwC analysts have seen a rise in human-operated ransomware and data exfiltration attacks.[3] These are attacks where the threat actor - usually motivated to extort the victim of cash payments in the form of cryptocurrencies - will not only deploy ransomware on the target, but will stage a lengthy reconnaissance process beforehand, extracting valuable and oftentimes confidential information from the target.

This information is used as leverage against the target once the ransomware is deployed, with threat actors now following through on their threats, releasing the victim's confidential files onto 'leak sites'. As of 20th May 2020, PwC has observed over 150 organisations around the world having had their data leaked in this manner by multiple threat actors.

Whilst it is difficult to directly attribute this activity to the COVID-19 pandemic, the statistics support the hypothesis that the increase in publicly known threat actor activity is a direct result of the current economic downturn. Of the incidents observed by PwC, over 60% of these occurred after the World Health Organisation's (WHO) declaration that COVID-19 was a pandemic. Of these, over 80% of incidents occurred after the UK went into an official lockdown on 24th March 2020.

With the AWM sector being a lucrative target before individual countries began instigating their national lockdown policies, the abrupt adoption of remote working technologies alongside threat actors growing more emboldened, presents new cyber security challenges at this time.

[3] PwC, 'Why has there been an increase in cyber security incidents during COVID-19?', https://www.pwc.co.uk/issues/crisis-and-resilience/covid-19/why-an-increase-in-cyber-incidents-during-covid-19.html

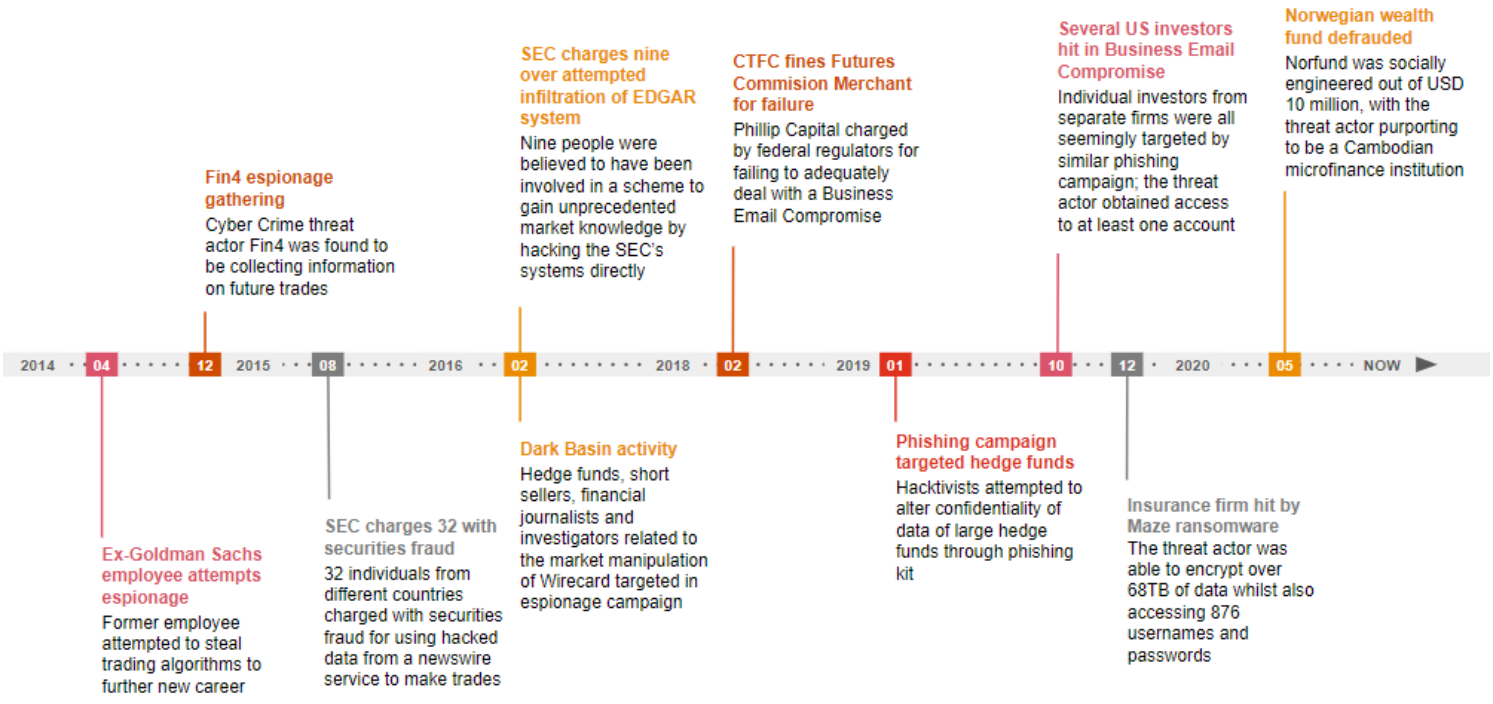
Timeline of attacks

The AWM sector has seen consistent targeting over the past decade; in the timeline graphic below, we detail some of the more recent and pertinent attacks to the sector.

Within the AWM sector sit many confidential and high-profile assets, all of which attract the attention of threat actors. The threat actors targeting the sector range in their motivations, but also vary in sophistication - from individual, insider threat attacks that could be classed as "low resourced", through to persistent, highly targeted state-sponsored threat actors which seek to obtain information from specific organisations.

A detailed explanation on how we categorise threat actors by motivation is located in Appendix 1 of this report.

> *'The Financial and Insurance sector has always had a target on its back due to the kinds of data it collects from its customers.'*
>
> Verizon DBIR Report, 2020



Incident themes

Based on past incidents and sector trends, we assess that the AWM sector is primarily a target for attackers motivated with criminal and espionage intent. Historically, the sector has been the target of espionage attacks due to the amount of non-public information that can be used by attackers to increase their own profits, often using this information to manipulate the markets. In this way, the AWM sector is unique in that an attacker's motivation can be somewhat interchangeable between crime and espionage.

However, with the threat of ransomware increasing across all sectors, as well as the AWM sector being subject to multiple Business Email Compromise (BEC) attacks over the more recent period, it is PwC's assessment that crime poses the largest threat to AWM-based organisations.

Criminal

With the AWM sector being responsible for significant capital, many organisations that sit under its umbrella make attractive targets for cyber criminals. Financial gain is a primary motivation for criminal threat actors, however, there are a multitude of means through which this can be achieved - whether that be financial crime, or the theft of data that can be easily monetised. The 'cyber' element of such attacks allows them to be conducted with lower risk, higher reward and variable modus operandi.

The shift to new technologies within the sector, such as the increased turn towards virtual currency, has created new and innovative avenues for cyber criminals to exploit. The overall rise in ransomware activity across 2020, with a particular spike observed during the COVID-19 pandemic, is a threat that must be considered for all sectors.

Direct financial gain

Many of the organisations that exist within the AWM sector include those that handle significant monetary transactions (e.g. private equity, hedge funds, asset management). The lifecycle of these transactions presents numerous points at which a threat actor can exploit their target for financial gain.

One of the most prominent attack methods used to target investors is known as a Business Email Compromise (BEC). This involves a threat actor either imitating or hijacking a legitimate email account in order to defraud individuals or organisations through spear phishing. BEC is effective because it is often difficult to differentiate illegitimate emails or fraudulent transactions from the legitimate ones:

- In May 2020, a Norwegian wealth fund was targeted by a threat actor using an account in the name of a Cambodian microfinance institution, successfully managing to extract USD 10 million in "funding" from the target;[4] and,
- In December 2019, a social engineering intrusion spanning over eight years was disclosed by a court in New York, whereby the attackers tricked day traders and their financial advisors into liquidating securities and wiring cash from brokerages to them through a BEC attack.[5]

In addition to this, it is also possible for threat actors to bypass direct interaction with the use of "credential phishing" in order to obtain company credentials that could help them facilitate an illicit transaction. This technique has been observed within the AWM sector in the past, with organisations having their employees' details used in order to extract funds from their clients, under the guise of legitimate transactions.[6]

These credentials can be obtained through multiple vectors, the most common of which are the use of spear phishing, credential reuse or brute forcing, as has also been observed in recent cyber intrusions within the AWM sector.[7]

Exploiting the customer

As threat actors have evolved, they have also established sophisticated methods for obtaining customer credentials, bypassing the need to infiltrate organisations directly. For example, threat actors have been observed to create their own fake web pages as part of credential harvesting attacks that mimic a customer portal. Although the sophistication of these pages varies from campaign to campaign, PwC has

[4] 'Norway's Wealth Fund Loses $10m in Data Breach', Info Security, https://www.infosecurity-magazine.com/news/norways-wealth-fund-loses-10m-in/ (15th May 2020)

[5] 'Hackers allegedly emptied brokerage accounts with a simple email scam — here's how to protect yourself', CNBC, https://www.cnbc.com/2019/12/11/how-to-protect-your-brokerage-account-from-email-scams.html (12th December 2019)

[6] 'CFTC Fines Phillip Capital for Failure to Prevent a Cyber Attack That Resulted in the Theft of Customer Funds', Paul Weiss, https://www.paulweiss.com/media/3978895/23sep19-cftc-phillip.pdf (23rd September 2019)

[7] 'Cyber Attack Hits Prominent Hedge Fund, Endowment, and Foundation', Institutional Investor, https://www.institutionalinvestor.com/article/b1hqqxdl6pf03f/Cyber-Attack-Hits-Prominent-Hedge-Fund-Endowment-and-Foundation (October 24th 2019)

observed several of these illegitimate credential phishing pages that look no different to the website they are attempting to spoof.

This type of attack can include the creation of fake mobile applications that mimic legitimate ones used by customers of an organisation. This attack vector in particular has been seen targeting users of banking and trading apps, with threat actors gaining full access to devices that download the illegitimate apps.[8]

New technologies, new problems

With the AWM sector being one of the more technologically mature, usually always embracing new technologies as they are made available, it is no surprise that there has been much in the way of innovation seen over the last few years.

One of the most disruptive is the introduction and embracing of virtual currencies. This has allowed AWM funds to diversify their portfolios, using virtual currencies to both invest into newer markets and to provide a new investment service for people using these virtual currencies.

However, with the implementation of technologies comes the risk of disruption, and the creation of new attack vectors. In one particular instance, an investment fund that used virtual currencies had a vulnerability in the system that transferred virtual tokens between members, allowing attackers to siphon off roughly 3 million tokens into their own organisation's account.[9] In 2014, JP Morgan experienced an attack resulting from a security oversight in the implementation of a new server, which led to the theft of around 83 million customer records by hackers.[10]

In the current climate, where organisations are adjusting to new remote working practices, it is particularly important for organisations to be cautious when implementing new protocols and technologies.

Ransomware

Across all sectors and industries, ransomware is an increasingly prominent threat. The AWM sector houses large amounts of information on confidential transactions, making it a prime target[11] for new variants of ransomware (e.g. Ragnar Locker) known to steal information from the target, as well as encrypt files. Previous cases of this in practice include:

- Canadian Insurance firm Andrew Agencies was struck with a variant of Maze ransomware in December 2019, where the threat actor supposedly encrypted 68TB of data whilst also stealing and exfiltrating the usernames and passwords of 876 users from the network;[12] and,
- Two Canadian banks were subjected to a ransomware attack in May 2018 that stole a total of 90,000 customer details (including social insurance numbers, dates of birth, and other personal information) whilst also asking for a USD 1 million payment.[13]

In addition to ransomware, Distributed Denial of Service (DDoS) extortion can be used to extort organisations by disrupting access to networks and online services. By way of an example, in 2017, several Malaysian banks and brokerages had their online share trading accounts held to ransom by a persistent attack that continuously shutdown the platform by repeatedly flooding the network with traffic in a DDoS extortion attack.[14]

As organisations adjust to the new business climate brought about by the COVID-19 situation by adopting working from home practices, it is worth noting that the impact of any successful attack may be increase as a result. As was seen in June 2020, the multi-national car manufacturer Honda was hit with a variant of Ekans ransomware. In addition to halting EU production lines, the effects of the attack were exacerbated by the large number of employees working from home at the time.[15] Furthermore, infrastructure pivotal for remote working, such as VPNs, could become an increasingly popular target for those seeking to disrupt business operations.

Espionage

As organisations within the AWM sector are privy to a vast amount of sensitive data, including corporate transactions and deals, they are likely to be of interest to both nation state threat actors and competitors. The sector is becoming

[8] 'Infostealer, Keylogger, and Ransomware in One: Anubis Targets More than 250 Android Applications', Cofense, https://cofense.com/infostealer-keylogger-ransomware-one-anubis-targets-250-android-applications/#1580849051168-d3690a62-9a7e (5th February 2020)

[9] 'Hack attack drains start-up investment fund', BBC News, https://www.bbc.co.uk/news/technology-36585930 (21st June 2016)

[10] 'JPMorgan data breach entry point identified: NYT', Reuters, https://www.reuters.com/article/us-jpmorgan-cybersecurity/jpmorgan-data-breach-entry-point-identified-nyt-idUSKBN0K105R20141223 (23rd December 2014)

[11] 'Ragnar Locker's well-conceived ransomware attack on Energias de Portugal', SC Media, https://www.scmagazine.com/home/security-news/ransomware/ragnar-lockers-well-conceived-ransomware-attack-on-energias-de-portugal/ (16th April 2020)

[12] 'Ragnar Locker's well-conceived ransomware attack on Energias de Portugal', SC Media, https://www.scmagazine.com/home/security-news/ransomware/ragnar-lockers-well-conceived-ransomware-attack-on-energias-de-portugal/ (16th April 2020)

[13] 'BMO and CIBC-owned Simplii Financial reveal hacks of customer data', CBC, https://www.cbc.ca/news/business/simplii-data-hack-1.4680575 (28th May 2018)

[14] 'No bitcoin payment to hackers', The Malaysian Reserve, https://themalaysianreserve.com/2017/07/10/no-bitcoin-payment-hackers/ (10th July 2017)

[15] 'Carmaker Honda targeted in cyber attack', Financial Times, https://www.ft.com/content/da60f3da-9669-4d50-ac33-144adac28f4b (9th June, 2020)

increasingly competitive, making intelligence gathering activities attractive for those who could use the information to gain a competitive market edge.

Espionage-motivated attacks within the AWM sector present themselves in a variety of different forms and through a number of unique attack vectors, and are likely to remain prevalent due to the perceived large gains to be made in possessing non-public knowledge. In 2020, an extensive campaign targeting hedge funds, short sellers and journalists connected to market manipulation was uncovered.[16] This activity was attributed to the India-based threat actor, Dark Basin (*a.k.a.* Orange Abtu), which PwC has tracked since 2018.

Gathering Information on future transactions

AWM is a primary target for espionage-based threat actors due to the fact that it is a sector that consists of many confidential and high-profile transactions. These transactions can have an impact on global stock markets and overall company share value, and any prior knowledge into these deals could make for a large financial gain for either rival firms or individuals operating in the same market. This would most likely be done by the threat actor embedding themselves into a company's network or email server, or through hacking trading systems directly.

This type of criminality connected with espionage activity has historically been extremely prevalent in the AWM sector, with the US Securities and Exchange Commission (SEC) alone dealing with multiple cases of intrusion into federal systems in order to gain non-public knowledge to enhance future trades:

- **Securities and Exchange Commission v. Dubovoy, et al -** the SEC charged 32 individuals with securities fraud for trading on hacked press releases, obtained through the successful attack of a newswire service that led to the theft of hundreds of corporate earnings releases before public release;[17]
- **Securities and Exchange Commission v. Zavodchiko, et al -** charges presented to nine individuals for securities fraud, using the same illegally acquired information from the previous case;[18] and,
- **SEC charges nine with hacking of EDGAR system –** the SEC brought new charges upon nine individuals for a securities fraud, similar to the previous cases. This time however, the attack was initially staged by intruding on the SEC's own Electronic Data Gathering, Analysis, and Retrieval (EDGAR) system, and then using this information to create trades off the back of non-public information.[19]

Within the sector, proprietary data such as investment research, predictive models and algorithms underpin the competitive edge of an organisation. As such, this type of data carries a high-value to competitors. Historical incidents affecting the sector have often been enabled by an insider element due to the level of access and specialist knowledge required:

- In 2014, a former Goldman Sachs employee reverse engineered the algorithms used by the large hedge fund to make trades, in order to further his own career. Although arrested and charged before being able to use the information, the intellectual property he stole was estimated to be worth USD 30 million;[20] and,
- In 2009, Citadel launched criminal proceedings against two former employees for industrial espionage, as they were found to have been using their former employer's trading algorithms for their newly created firm, Teza Technologies.[21]

Sabotage

Destructive attacks with the aim of sabotaging business can be motivated by a variety of factors including those seeking political or economic gains. Sabotage threat actors could seek to corrupt systems and cripple operational capabilities, for example, by completely erasing business-critical data. This could be achieved via the use of ransomware or wiper malware, deployed either to directly sabotage operations, or as a final act to obscure the threat actor's activity on the victim's system.

There is also an increasing trend towards the use of destructive malware as a diversion - drawing attention away from the threat actor's ultimate target. In 2018, Banco de Chile's networks were compromised with a wiper malware.

---

[16] 'Uncovering a Massive Hack-For-Hire Operation', Citizen Lab, https://citizenlab.ca/2020/06/dark-basin-uncovering-a-massive-hack-for-hire-operation/ (9th June 2020)

[17] 'Securities and Exchange Commission v. Dubovoy, et al., Civil Action No. 2:15-cv-06076-MCA-MAH (D.N.J. filed Aug. 10, 2015) (amended Aug. 23, 2015)', SEC, https://www.sec.gov/litigation/litreleases/2015/lr23319.htm (13th August 2015)

[18] 'Securities and Exchange Commission v. Zavodchiko, et al., Civil Action No. 2:16-cv-00845-MCA-LDW (D.N.J., filed February 17, 2016)', SEC, https://www.sec.gov/litigation/litreleases/2016/lr23471.htm (18th February 2016)

[19] 'SEC Brings Charges in EDGAR Hacking Case', SEC, https://www.sec.gov/news/press-release/2019-1 (15th January 2019)

[20] 'The Triple Jeopardy of a Chinese Math Prodigy', Bloomberg, https://www.bloomberg.com/news/features/2018-11-19/the-triple-jeopardy-of-ke-xu-a-chinese-hedge-fund-quant (19th November 2018)

[21] 'Banco de Chile Wiper Attack Just a Cover for $10M SWIFT Heist', ThreatPost, https://threatpost.com/banco-de-chile-wiper-attack-just-a-cover-for-10m-swift-heist/132796/ (13th June 2018)

This activity was subsequently found to be a distraction for a SWIFT heist resulting in the theft of USD 10 million by a North Korea-based threat actor PwC tracks as Black Artemis.[22] NotPetya is an example of destructive malware which masqueraded as ransomware.[23] This affected many organisations on a global scale in 2017, indiscriminate of sector.

DDoS is another method used for disrupting business operations, and this is one of the most accessible types of attack available to threat actors to achieve this objective. For organisations within AWM, a disruption to networks could significantly affect online customer services and real-time activities, such as the ability to perform real-time investment trading.

Several brokerages have been targeted in this manner with varying levels of success. For example, in 2019, Singapore-based brokerages were targeted by DDoS attacks resulting in minor disruption to trading platform access.[24]

A long-term strategy to damage business could be employed to alter influential data sets over time, impairing decision-making capabilities by undermining data integrity. An attack which, for example, successfully alters proprietary investment algorithms would be particularly concerning because it could go unnoticed for some time and result in significant financial loss both to the affected organisation and its clients.

Hacktivist

Although many organisations within the AWM sector maintain a relatively low profile, the perception of large profits and the wealth of its clients may, on occasion, catch the attention of anti-capitalists. This activity can be fuelled by negative news stories in the media, irrespective of their legitimacy. For example, associations with tax havens, or controversial investment portfolios with funds negatively associated with climate change, weapons manufacturing or third world debt, could serve to motivate hacktivists.

Hacktivist activity typically seeks to raise awareness of the hacktivist's cause. This commonly manifests in the form of website defacements or DDoS attacks. Although these are often low impact in nature, these incidents can cause a loss of confidence in the ability of the affected organisation to effectively secure customer data:

- In 2019, BlackRock was victim to a spoofing campaign in which a fake letter concerning the company's climate change strategy was published under the name of its CEO and sent to journalists;[25] and,
- The 2018 Future Investment Initiative (FII) conference based in Saudi Arabia had its website defaced prior to the start of the event. The attack appeared to be politically motivated.[26]

More technically sophisticated hacktivists may also seek to steal and divulge sensitive data or otherwise disrupt operations, crossing over into the sabotage domain. For example, a hacktivist launched a phishing campaign in 2019 to target international hedge funds with the intention of compromising their data confidentiality. It is still unclear whether any of these attacks were successful.[27]

---

[22] 'Banco de Chile Wiper Attack Just a Cover for $10M SWIFT Heist', ThreatPost, https://threatpost.com/banco-de-chile-wiper-attack-just-a-cover-for-10m-swift-heist/132796/ (13th June 2018)

[23] 'The Untold Story of NotPetya, the Most Devastating Cyberattack in History', Wired, https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/ (22nd August 2018)

[24] 'Some brokerages in Singapore hit by DDoS attacks last week', The Business Times, https://www.businesstimes.com.sg/banking-finance/some-brokerages-in-singapore-hit-by-ddos-attacks-last-week (30th October 2019)

[25] 'The Fake Larry Fink Letter That Duped Reporters', Institutional Investor, https://www.institutionalinvestor.com/article/b1cqj0xmn5ds9t/The-Fake-Larry-Fink-Letter-That-Duped-Reporters (16th January 2019)

[26] 'Saudi Arabia's 'Davos in the Desert' website was hacked and defaced', TechCrunch, https://techcrunch.com/2018/10/22/saudi-future-investments-conference-site-hacked-defaced-jamal-khashoggi/ (22nd October 2018)

[27] 'Phisher Announces More Attacks Against Hedge Funds and Financial Firms', Bleeping Computer, https://www.bleepingcomputer.com/news/security/phisher-announces-more-attacks-against-hedge-funds-and-financial-firms/ (1st March 2019)

Case studies

The below case studies provide an overview of publicly-reported attacks that have taken place in recent years. These examples also illustrate the wide-ranging motivations of the threat actors which have targeted the AWM sector.

1. Norwegian state-owned wealth fund defrauded out of USD 10 million

Threat Actor Motivation	Target	Year
Criminal	Wealth fund	2020

A cyber criminal enterprise posing as a Cambodian microfinance institution managed to elicit payments totaling USD 10 million from the Norwegian state-owned investment fund, Norfund. The criminals successfully falsified information exchange between Norfund and the so-called "Cambodian institution", such that the wealth fund was not made aware of the scam until a month after the initial transaction had been completed, when the threat actor reappeared, looking to recreate the scam.[28]

2. Insurance firm hit by Maze ransomware

Threat Actor Motivation	Target	Year
Criminal	Insurance broker	2019

The Canadian Insurance firm Andrew Agencies was subject to a Maze ransomware attack. According to the threat actor, it was able to encrypt over 68TB of data, whilst also accessing and exfiltrating 876 usernames and passwords from the network.[29]

3. US Investors hit with Business Email Compromise (BEC) attack

Threat Actor Motivation	Target	Year
Criminal	Hedge fund	2019

US-based hedge fund Arena Investors was an intended victim in a larger campaign targeting institutional investors (two other investment executives from separate firms were also targeted). The attack came in the form of a spear-phishing email, which allowed the attackers to gain control of the desired accounts. Whilst there was no altering of any funds, with no illicit transactions made, it is likely the attackers were looking to use the legitimate company emails as a stager to send out further spear phishing links to other companies.[30]

4. Phishing campaign targeted hedge funds

Threat Actor Motivation	Target	Year
Hacktivism	Hedge funds	2019

A phishing campaign known as 'Beyond the Grave' targeted international hedge funds in 2019. A hacktivist claimed the phishing kit was designed to alter the data confidentiality of hedge funds and claimed to have compromised several companies including Elliot Advisors, Capital Fund Management, AQR, Citadel, Baupost Group and Marshall Wace. It posted images to show the deployment of phishing emails, although it is still unclear whether any of these were actually successful. The emails impersonated a legitimate

[28] 'Norway's Wealth Fund Loses $10m in Data Breach', Info Security, https://www.infosecurity-magazine.com/news/norways-wealth-fund-loses-10m-in/ (15th May 2020)

[29] 'Canadian Insurance Firm Hit By Maze Ransomware, Denies Data Theft', Bleeping Computer, https://www.bleepingcomputer.com/news/security/canadian-insurance-firm-hit-by-maze-ransomware-denies-data-theft/ (18th December 2019)

[30] 'Cyber Attack Hits Prominent Hedge Fund, Endowment, and Foundation', Institutional Investor, https://www.institutionalinvestor.com/article/b1hqqxdl6pf03f/Cyber-Attack-Hits-Prominent-Hedge-Fund-Endowment-and-Foundation (24th October 2019)

financial research company, with topical content related to the European Securities and Markets Authority (ESMA) suspending short selling during Brexit.[31]

5. CTFC fines Futures Commission Merchant for failure to prevent the stealing of customer funds

Threat Actor Motivation	Target	Year
Criminal	Wealth fund	2018

The Commodity Futures Trading Commission (CTFC) fined Phillip Capital, a Futures Commission Merchant, for failing to prevent a BEC that allowed the attacker to obtain customer information that saw the illicit transfer of USD 1 million from a customer's account to the attackers. Although the firm's internal security team noticed the breach, it did not, according to the CTFC, proceed to deal with the incident in an acceptable manner, allowing the attacker to remain on the system and carry out the attack.[32]

6. Dark Basin activity

Threat Actor Motivation	Target	Year
Espionage	Hedge fund, short sellers, journalists, investigators	2016

Dark Basin (*a.k.a.* Orange Abtu) is a hacker-for-hire group that has targeted victims across multiple sectors and geographies. This activity has included financial sector targets. Hedge funds, short sellers, financial journalists and investigators were likely targeted in connection to market manipulation activity at the German payment processor, Wirecard AG. Private emails were leaked via the Zattara Leaks site as part of this activity.[33]

7. SEC charges nine over attempted infiltration of EDGAR system

Threat Actor Motivation	Target	Year
Espionage	Securities and Exchange Commission	2016

A group of cyber criminals originating from Ukraine were found guilty of hacking into the US Security and Exchange Commission's (SEC's) EDGAR system and extract non-public information for illegal trading. The intrusion took place sometime in early 2016, with the perpetrators earning an estimated USD 4.1 million in illicit profits over 157 separate trades.[34]

8. SEC charges 32 with securities fraud

Threat Actor Motivation	Target	Year
Espionage	Hedge funds	2015

The SEC charged 32 individuals for using hacked press releases from a newswire service to make illegal trades. The press releases, numbering in their hundreds, revealed corporate earnings that had not yet been disclosed publicly. The individuals involved ranged

[31] 'Phisher Announces More Attacks Against Hedge Funds and Financial Firms', Bleeping Computer, https://www.bleepingcomputer.com/news/security/phisher-announces-more-attacks-against-hedge-funds-and-financial-firms/ (1st March 2019)

[32] 'CFTC Fines Phillip Capital for Failure to Prevent a Cyber Attack That Resulted in the Theft of Customer Funds', Paul Weiss, https://www.paulweiss.com/media/3978895/23sep19-cftc-phillip.pdf (23rd September 2019)

[33] 'Uncovering a Massive Hack-For-Hire Operation', Citizen Lab, https://citizenlab.ca/2020/06/dark-basin-uncovering-a-massive-hack-for-hire-operation/ (9th June 2020)

[34] 'SEC Brings Charges in EDGAR Hacking Case', SEC, https://www.sec.gov/news/press-release/2019-1 (15th January 2019)

in country of origin from the US, France, Cyprus, Russia, and Ukraine.[35] In September 2015, the SEC added two more people to be charged for this event.[36]

9. Fin4 espionage gathering for future trades

Threat Actor Motivation	Target	Year
Espionage	Mergers and Acquisitions (M&A)	2014

A threat actor was observed targeting multiple individuals all possessing non-public information about merger and acquisition (M&A) deals and other major changes to the markets. The group targeted multiple organisations, from regulatory risk to legal counsel, gathering information about upcoming deals and completed deals that were not yet public knowledge.[37]

10. Ex-Goldman Sachs employee attempts espionage

Threat Actor Motivation	Target	Year
Espionage	Goldman Sachs	2012

A former Goldman Sachs employee, looking to start a new trading career in Asia, reverse engineered his employer's trading algorithms to take to his new job. The assets, estimated by Goldman Sachs to be worth roughly USD 30 million, were stored in various laptops that the employee had given to his family in mainland China and Hong Kong.[38]

[35] 'Securities and Exchange Commission v. Dubovoy, et al., Civil Action No. 2:15-cv-06076-MCA-MAH (D.N.J. filed Aug. 10, 2015) (amended Aug. 23, 2015)', SEC, https://www.sec.gov/litigation/litreleases/2015/lr23319.htm (13th August 2015)

[36] 'Litigation Release No. 23345 / September 14, 2015: Securities and Exchange Commission v. Dubovoy, et al., Civil Action No. 2:15-cv-06076-MCA-MAH (D.N.J., filed August 10, 2015)', SEC, https://www.sec.gov/litigation/litreleases/2015/lr23345.htm (15th September 2015)

[37] 'Hacking the street? Fin4 likely playing the market', FireEye, https://www2.fireeye.com/rs/fireye/images/rpt-fin4.pdf

[38] 'The Triple Jeopardy of a Chinese Math Prodigy', Bloomberg, https://www.bloomberg.com/news/features/2018-11-19/the-triple-jeopardy-of-ke-xu-a-chinese-hedge-fund-quant (19th November 2018)

Conclusion

Organisations that sit within the AWM sector have historically been a lucrative target for threat actors, due in large part to the sheer amount of assets and capital that they control. Whether it be from espionage attacks that look to exploit confidential information in regard to high-stake trades or deals, or criminal attacks for direct financial gain, the AWM sector makes an attractive target.

Based on incident trends, case studies of attacks, and the external forces that are currently influencing a spike in ransomware activity, PwC assesses that cyber criminal threat actors pose the greatest threat to the AWM sector. The sophistication of cyber criminal threat actors varies considerably, with those on the higher end of the scale reaping in millions. On the other hand, low-level tools, techniques, and procedures used against AWM organisations, to facilitate ransomware attacks, and DDoS extortion, are still met with success.

However, the threat of espionage on the AWM sector is the most historically prevalent of the attacker motivations, and so must be viewed as being no less prominent a threat than cyber crime. As there is always potentially a large amount to be gained in profiting off of illicit activity within the AWM sector, such as stealing and re-using trading algorithms, or using non-public information in order to make lucrative trades, the motivation for espionage-based attacks for financial gain is still extremely high.

Sabotage attacks are not beyond the purview of threat actors targeting the AWM sector and represent a tangible danger to organisations within the sector. On the lower end of the scale, DDoS attacks can be leveraged to cause disruption to both internal and customer-facing services. Although rare in nature, destructive malware could be utilised to destroy victim systems resulting in a catastrophic impact to business and having an ultimate impact on the bottom line.

While hacktivism threats are often low-impact in nature, the sector attracts the attention of anti-capitalist threat actors from time-to-time. As threat actors operating in this space begin to have more sophisticated tooling at their disposal, this is an area which could present a larger threat in the future.

Knowing which threat actors are relevant to a given sector is an important step toward strategically directing investment in appropriate defences. The overall view presented in this report, however, spans the entire AWM sector, and more granular threat analysis should be done on a per-organisation basis. Analysis of how threats would navigate your organisation's infrastructure to achieve their objective can help to identify the gaps that exist in your security controls, and enable you to tailor your preparation efforts appropriately.

Appendix 1: Analysis methodology

Most cyber attacks have an underlying and ultimate motivation. Although attacks by separate threat actors might share objectives, separate threat actors do not always share the same motivation. Examining the motivation of an attack can enable the identification of the category of attacker.

PwC divides the threat landscape according to the motivation of those behind cyber attacks. For each, some common tactics, techniques, and procedures (TTPs) observed by PwC's Threat Intelligence team are included. The divisions are as follows.

Motivation	Description
 **Criminal** For the money	Cyber criminals are largely indiscriminate in who they attack as they simply seek to monetise their attacks. The range in sophistication of cyber criminals is vast, and displays a widely different set of Tools, Techniques and Procedures (TTPs). Low-level criminals may look to use credential phishing or Business Email Compromise (BEC) schemes in order to trick organisations into either providing them access to customer funds, or into sending payment to them directly. These types of activity still exist at the more sophisticated end of the spectrum, but these actors will also employ more advanced techniques, such as ransomware. These types of malware have become more and more sophisticated over time, with the ability to not just encrypt organisations' files and hold those to ransom, but to also, in some cases, steal confidential data and subsequently sell it to the highest bidder through their bespoke leak-sites.
 **Espionage** For the motivation	Espionage threat actors (often referred to as "Advanced Persistent Threats", or APTs) typically seek to steal information which will provide an economic or political advantage to their benefactor. Attacks motivated by espionage usually originate from either industry competitors or state-sponsored threat actors. Often the benefactor is a nation state, and espionage activity aligned to state objectives will reflect geopolitics and real-world events. Usually, the information sought out by espionage attackers is only found at specific organisations, meaning they repeatedly target the same organisation and their suppliers until they have completed their mission.
 **Sabotage** For the impact	Saboteurs seek to damage, destroy or otherwise subvert the integrity of data and systems. Sabotage attacks are not always deliberate and have been used to mask other malicious activity. Sabotage operations designed to be a diversion can still result in significant collateral damage. Examples of attacks include wiping hard drives, causing SCADA systems to malfunction or altering trade data. As with espionage attacks, attacks from saboteurs tend to be influenced by real-world events, making the risk of attacks specific to geography and company actions in relation to political events/issues.
 **Hacktivist** For the cause	Hacktivists conduct attacks to increase their public profile and raise awareness of their cause .This is typically done through the disruption of services such as denial of service (DoS) attacks, and website defacements. In many cases such attacks are random; they care little how this is done or who is affected, so long as their message is promoted. In some cases, however, their victims are targeted, due to an organisation or individual's perceived actions or support of an issue. As with espionage, attacks from hacktivists are sometimes influenced by real-world events, meaning the risk of such attacks is subject to change.

Appendix 2: PwC Threat Intelligence

About Us

PwC is globally recognised as a leader in cyber security and as a firm with strong global delivery capabilities and the ability to address the security and risk challenges our clients face. We underpin our board-level security strategy and advisory consulting services with expertise gleaned from the front lines of cyber defence across our niche technical expertise in services such as red teaming, incident response and threat intelligence.

Our threat intelligence team specialises in providing the services which help clients resist, detect and respond to advanced cyber-attacks. This includes crisis events such as data breaches, economic espionage and targeted intrusions, including those commonly referred to as APTs. We differentiate ourselves with our ability to combine strong technical capabilities with strategic thinking, with our research conducted by our in-house experts recruited primarily from governments, the military, and the security services- giving us a unique perspective and a vast array of contacts.

We offer a range of threat intelligence products and services designed to enable an effective defence against advanced cyber threats.

Cyber threat intelligence subscription

Access to PwC's targeted attack indicator feeds, network and endpoint signatures and tactical and strategic reporting.

Directed research and assessments

Direct access to PwC's threat research team for tasks relating to ad-hoc or long term enquiries – both tactical and strategic research into malicious samples, threat actors or analysis support.

Cyber threat intelligence monitoring

Continuous, bespoke and focused research which would augment our subscription services.

Consulting and advisory

Advisory services to help organisations define requirements, consume, apply and produce threat intelligence in a way which best suits their organisation.

If you would like more information on our services, or to discuss any of the threats contained in this report please feel free to get in touch at chris.eaton@pwc.com.

How can PwC help?

As the international response continues to develop, we know that organisations across the Channel Islands are facing significant cyber security challenges to which they need to respond rapidly; our experienced and expert team can work alongside you to tackle these.

Mike Byrne
Asset & Wealth Management leader,
PwC Channel Islands
Tel: +44 7700 838278
Email: michael.j.byrne@pwc.com

Christopher Eaton
Director, Advisory Services,
PwC Channel Islands
Tel: +44 7700 838349
Email: chris.eaton@pwc.com

Volodymyr Kazanskyi
Senior Manager, Advisory Services,
PwC Channel Islands
Mobile: +44 7797 776404
Email: volodymyr.kazanskyi@pwc.com

pwc.com/jg/en/cyber