Modernizing the fight against financial crime: Exploring the Evolving Challenges of Cyber-Financial Crime Through Partnerships and Technology

By Standard Chartered Bank – October 2018

Introduction

Criminal groups are increasingly leveraging online capabilities as a means of supplementing traditional illicit techniques, such as money mule networks. They do this by either employing individuals with technical skills (the use of Cyber-as-a-Service) or by increasing their own capabilities. This expanding nexus between cyber and 'traditional' criminal activities means that suspicious financial activity will often have both a cyber element (e.g. the use of cryptocurrencies to launder illicit proceeds) and a traditional element (e.g the use of money mules to move and convert illicit proceeds). Cyber criminals continue to seek new methods to 'cash out' their ill-gotten financial gains and, while often moving swiftly to adopt new technologies, will still need to place these funds back into the financial sector. The knowledge and understanding Banks have of the financial system is a crucial component in understanding the overall picture of cyber criminals' activity. The agility of cyber criminals and the pace of change in new technologies places an increased importance on public-private sector collaboration in order to better understand and combat these ever evolving threats. We believe banks, industry, government, and law enforcement need to continue working together to explore, leverage, and develop new and better tools, skills and frameworks to tackle illicit activity and recover the proceeds of crime.

Cyber Financial Intelligence

Standard Chartered's Cyber Financial Intelligence Unit (CyFI) was set up to investigate the misuse by cyber criminals of the financial system. It is building a cyber toolbox, crucial for tackling advanced cyber related criminal activity. An example is CyFI's use of blockchain analysis tools. Criminals use virtual and/or cryptocurrencies to launder illicit proceeds. This poses a challenge to traditional Financial Crime Compliance techniques as funds are moved outside the traditional financial sector as well as between various currencies. However, in the case of Bitcoin (BTC), transactions are published on a public ledger. While BTC transactions are designed to be "pseudonymous", CyFI is piloting the use of advanced blockchain analysis tools to help peel back the layers of transactions and flows, revealing key pieces of information about the parties involved as well as other vital threads. Additionally, CyFI's uses advanced analytics to scan the dark web (underground criminal sites) for open source intelligence on "wallets", which are accounts where BTC can be transferred in and out. Piecing together information about these wallets adds depth to our intelligence regarding the parties involved, as well as the nefarious activity flowing to and from various Darknet Markets. Often our work identifies a nexus between Cyber Financial Crime and more traditional criminal techniques, highlighting why following the money still matters. For example, money mule networks play a critical role in cyber related crimes. Interpol estimates that 90% of money mule activity is associated with cyber-enabled or cyber-dependent crime. Professional money laundering networks specialise in the transfer of illicit proceeds from criminal acts. Money mules are recruited and managed by mule herders, who provide specialised services to other Organized Crime Groups. Although the use of money mules is a traditional laundering technique, herders often advertise their services on the Dark Web and take a percentage of the illicit proceeds as commission. CyFI is working with law enforcement on several cases through the National Cyber Forensic Training Alliance (NCFTA), a neutral, non-profit that enables government, academia and private industry to identify, disrupt and mitigate cyber crime. CyFI utilizes various techniques to identify potential mule herders through transactional analysis and data collected by NCFTA from other partners.

> ***"It is simply not possible to have success without the cooperation and collaboration of both industry and government. The problem is global in nature and impacting all sectors, thus our approach requires a totality of effort."***
>
> Steve Mancini | Chief Technology Officer | NCFTA

How GozNym Malware Proceeds Moved through Money Mule Networks

Meeting the Evolving Challenges of Cyber-Financial Crime Through Partnerships and Technology

Case Study: The Ripple Ransomware Attack

On 27 May 2018, a cyber threat actor demanded a total of 2 million Canadian dollars ($1.54 million USD) in ransom from two Canadian banks, BMO (Bank of Montreal) Financial Group and Simplii Financial. A combined 90,000 customer credentials were allegedly compromised including account numbers and passwords. The cybercriminal threatened to expose customer information if the ransom was not paid. The ransom was to be paid in XRP tokens, the currency of the Ripple cyptocurrency network. Whilst there is no reporting to indicate a payment has been made by either bank, compromised credentials have yet to appear on Darknet Markets. This is one of the first occasions that a ransom has been extorted in altcoin (an alternative cryptocurrency to BTC).

A Ripple in the Water: Why XRP?

On the day of the incident, BTC closed at $7,368.22 USD while XRP closed at $0.607881 USD. Although demanding BTC could be more lucrative and possibly easier to move than XRP, the cybercriminals likely made a deliberate choice to use a less well-known cryptocurrency. Currently, BTC's market capitalization is approximately 125% higher compared to the next five largest cryptocurrencies combined. As a result, law enforcement investigations associated with cryptocurrencies would mostly focus on BTC. The hackers may have believed that law enforcement would not have the same level of experience or tools to investigate altcoins as they did for BTC. This may explain why they demanded the ransom payment in XRP. However, Ripple, has controls in place to monitor and report any AML flags across its network and, as a holder of a virtual currency license and registered MSB, would report suspicious activity to authorities.

External Partnerships and Emerging Technology

The CyFI team leveraged the partnership with the NCFTA in order to gain additional intelligence. Since the cryptocurrency demanded by the cybercriminals was XRP, and existing blockchain analysis tools mostly only focus on BTC or a limited number of other virtual currencies, the challenge to trace transactions was made more difficult. Along with increasing the number of virtual currencies that are included in their platforms, blockchain analysis tools are developing Know Your Transaction (KYT) services that will enable banks and exchanges to better monitor activity taking place on cryptocurrency blockchains. In the interim, CyFI is able to follow XRP and other selected altcoin (Ethereum and Litecoin) transactions through the use of a range of blockchain tools and other fusion analysis. Using such tools and working with law enforcement, enables CyFi to build intelligence on the entities, and accounts associated with the cybercrime.

Incidentally, although often thought of as a cryptocurrency, Ripple is also the name given to an alternative global payment infrastructure for banks. In December 2015, Standard Chartered Bank partnered with Ripple as part of its digitization agenda to produce innovative client solutions across businesses. This technology enables real-time fund settlement among global banks regardless of currencies, jurisdictions, and payment networks.

"CyFI produces intelligence through the fusion of financial data, cyber threat intelligence, web research, mining of restricted access sites, and much more. Working in collaboration with other internal teams, industry partners and law enforcement, CyFI plays a proactive role in identifying, mitigating and disrupting financial crime risks to the Bank from cyber-enabled and cyber-dependent crime."

Patricia Sullivan | Head Financial Crime Compliance Europe & Americas | Standard Chartered Bank

Strengthening Information Sharing

The benefits of information sharing are clear. However, to ensure continued trust, public-private partnerships have to balance what information can be shared with privacy and confidentiality requirements. Sharing non-client information, trends, patterns, public information, etc. is becoming the norm but we believe more can be done to increase information sharing. For example, CyFI continuously engages with various internal and external entities to navigate the information sharing protocols in order to maximize the information that can be legally shared. As such we continue to review legal frameworks surrounding cyber threat information sharing. Additionally, CyFI is working internally with our information security teams to share and expand information obtained from cyber incidents. Any information that can be appropriately shared, such as Indicators of Compromise (IOC), especially if it is beneficial for the industry and government to protect its infrastructure and/or to conduct enforcement actions as appropriate, will be shared, either directly or through the NCFTA. Continued engagement and collaboration among internal counterparts is in the spirit of FinCEN's 2016 guidance, 23 NYCRR 500, and other regulatory bodies that express the need for stronger collaboration between AML and cyber security units within a financial institution.