KPMG

Blockchain analytics tools offer new ways to 'follow the money' in ransomware cases

home.kpmg/blockchainanalytics

Evolving business models and the rapid global shift to remote working — combined with the growing use of cryptocurrencies — are creating new ransomware threats for businesses everywhere. While threats are on the rise, however, so is the use of powerful new capabilities in the form of blockchain analytics tools to combat today's costly trend.

A type of malicious software that can block access to computer systems or valuable data — typically paralyzing business-critical processes — ransomware is allowing cyber criminals to cash in as never before by extorting businesses large or small for cryptocurrency payments. But today's blockchain analytics experts are increasingly taking up the trail to 'follow the money', tracking the movement of illicit funds to provide solutions and new defenses. US investigators made an encouraging breakthrough in May, for example, tapping into the power of blockchain analytics and quickly recovering US$2.3 million of the US$4.4 million paid out in a well-publicized attack on US energy giant Colonial Pipeline Co.[1]

According to blockchain analytics firm Chainalysis,[2] ransomware-linked addresses extorted at least US$81 million in cryptocurrencies as of 10 May 2021, after amassing a record US$406 million in 2020. Chainalysis notes that the true toll is probably much higher, as corporations often fail to report costly ransomware attacks that are on the rise.

An estimated 41 percent of organizations have reported experiencing increased cyber-crime incidents, including ransom attacks, while employees have been working from home.[3] Cases continue to mount. Colonial Pipeline, operator of the largest US fuel pipeline, suffered a May 2021 ransomware attack that disrupted oil and gas supplies in the US, with the firm paying US$4.4 million in bitcoin to unlock its network.[4]

Recent data indicate that most ransomware victims are paying up in order to limit business disruption and damage. Global insurance firm Hiscox Group, in its 2021 *Cyber Readiness Report*, puts the figure at roughly 60 percent for impacted clients.[5] And paying doesn't guarantee anything near full recovery.

On average, ransom payers have recovered just 65 percent of their encrypted data, while 29 percent recovered only half of their data, according to a recent report by cyber-security firm Sophos — *The State of Ransomware 2021* — following a global survey of more than 5,000 organizations.[6] Sophos notes that 37 percent of businesses surveyed reported being hit in the last year by ransomware, which Sophos calls a 'major threat' to today's businesses.

1 Organized crime is cashing in

Ransomware attacks are also increasing in sophistication. Beyond encrypting data to paralyze businesses, hackers today often 'exfiltrate' or steal confidential or business critical data for ransom. If no payment is made, the data is leaked publicly. So-called 'commodity malware,' meanwhile, can appear in business systems as low-level malware but is designed to access a target, gather valuable data and share it with attackers to launch their extortion attempts.

In addition, the combination of cryptocurrencies and ransomware has created a powerful tool for organized crime groups. The reality is that ransomware is providing a high return on investment for criminals, and the rapid growth of liquidity in cryptocurrency markets is creating more opportunities for lucrative attacks on businesses.

[1] https://www.bbc.com/news/business-57394041
[2] https://blog.chainalysis.com/reports/ransomware-update-may-2021
[3] Harvey Nash/KPMG CIO Survey, 2020
[4] https://www.bbc.com/news/business-57394041
[5] Hiscox *Cyber Readiness Report*, https://www.hiscoxgroup.com/cyber-readiness
[6] Sophos *The State of Ransomware 2021*, https://secure2.sophos.com/en-us/medialibrary/pdfs/whitepaper/sophos-state-of-ransomware-2021-wp.pdf

2 Using blockchain analytics to 'follow the money'

Fortunately, blockchain analytics tools are increasingly being used by authorities and Virtual Asset Service Providers (VASP), companies providing services related to cryptoassets, and cryptoasset exchanges like Coinbase, to monitor transactions and detect questionable or revealing patterns related to ransom attacks. KPMG professionals also are deploying blockchain analytics tools today to help clients 'follow the money.'

Bitcoin is now the most-used cryptocurrency in attacks and considered the most-detectable of cryptocurrencies, ultimately making it easier for blockchain analytics tools to trace the steps taken by malicious actors.

Experts can take advantage of the fact that bitcoin is not completely anonymous but instead 'pseudo-anonymous.' Every transaction is visible on the public bitcoin blockchain, and while transaction data does not contain information about a sender's or receiver's true identity, bitcoin addresses can provide clues to identities.

Blockchain analytics providers aggregate information outside the blockchain — known as 'off-chain data' — in order to identify the senders and receivers of funds. To achieve this, analytics analyze historical blockchain data, combined with knowledge of good and bad actors and techniques, to detect transaction patterns. This makes it possible to identify the blockchain addresses of illicit actors and provides a critical opportunity to track illicit funds.

Laundered cryptocurrency typically makes its way — via crypto exchanges — to banks as criminals convert cryptocurrency to fiat currency. On their journey, criminals can use 'mixers' or non-compliant exchanges to cover their tracks, mixing their bitcoins with other users to make detection more difficult. Hackers can also go to peer-to-peer (P2P) platforms and exchange cryptocurrency with others to avoid authorities. Attackers also use a 'peel chain' pattern to obfuscate illicit funds — basically a chain of multiple bitcoin wallets that ransom funds pass through to conceal the trail of illegally obtained cryptocurrency.

3 Making progress to combat costly attacks

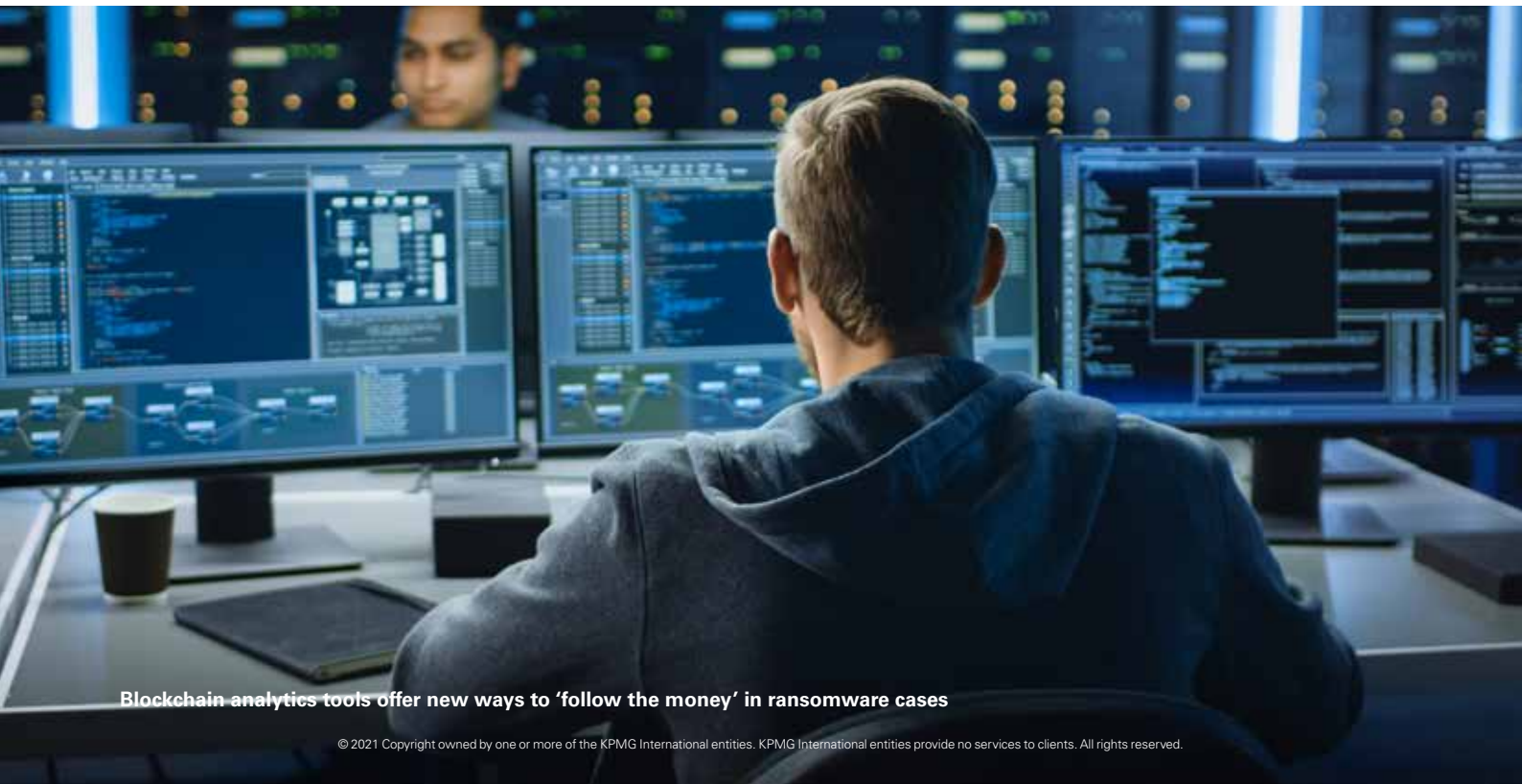
Fortunately, as is being seen, blockchain analytics tools — which are distinct from typical anti-money laundering techniques and systems — can help VASPs and authorities screen crypto wallets and transactions for connections to illicit activities. They also provide risk scores for the addresses users are interacting with, ideally allowing them to identify, manage and mitigate risk. This is helping businesses to prevent illicit funds from being laundered through their systems, or to detect such activity and report it to authorities.

As is being seen, blockchain tools drive progress in making ransomware attacks less attractive. US investigators managed to recover millions paid out in the May attack noted above on Colonial Pipeline. Within days of the ransom payment, blockchain analytics firm Elliptic identified the bitcoin wallet that received the payment and observed that it had received bitcoin payments since March and, although most of the payments were moved out, about US$2 million remained in the same account and was seized by the FBI.[7]

KPMG professionals are taking advantage of blockchain analytics tools to help clients identify 'dirty money' related to a ransom attack. They are working from different angles to help clients in this context:

— Helping VASPs and exposed financial institutions to design anti-money-laundering (AML) and counter-terrorism financing (CTF) models that allow the identification, detection and mitigation of risks associated with the entry of illicit funds.

[7] https://www.elliptic.co/blog/elliptic-follows-bitcoin-ransoms-paid-by-darkside-ransomware-victims



Blockchain analytics tools offer new ways to 'follow the money' in ransomware cases

— Integrating the functionality of blockchain analytics tools within the operational-monitoring function.

— Designing scenarios that allow the detection of potential risk patterns in the behavior of clients, and identifying links used to enable the receipt of funds related to a ransomware attack.

— Performing due diligence reports about the origin of illicit funds to assess their connection to ransomware attacks or the dark web.

4 Addressing the menace and today's growing threats

Research by Verizon indicates that up to 90 percent of ransomware campaigns work by targeting known vulnerabilities to gain initial access.[8]

It is also important to note how third-party risk is becoming significant. Changing suppliers in the event of an attack, or during pandemic-related supply-chain disruption, is often being fast-tracked without adequate rigor, creating new threats.

Such challenges have accelerated amid the massive increase in cloud-services adoption accompanying today's work-from-home trend. Cloud technology and tools providing instant access to business networks have been very convenient for businesses but also for potential attackers.

To make matter worse, ransomware as a service is increasing the efficiency of malicious actors. Essentially, someone packages a suite of tools used in an attack, allowing cyber criminals to surreptitiously encrypt data within the compromised organization and hold it ransom.

Ultimately, firms need to address, post-attack, precisely how an attack happened. But businesses too often assume that once a ransom is paid, the problem is solved — when in fact attackers often return with new extortion demands.

There is also a need for cryptocurrency exchanges to implement adequate controls. If bitcoins obtained by hackers go to an exchange, the exchange should have controls and anti-money-laundering measures in place to track and ideally identify illegally acquired bitcoins, or other crypto assets. Banks and VASPs should also heighten defenses and their capabilities to prevent money from ransomware attacks entering their platforms.

Businesses ideally need to enhance all defenses across the diverse attack vectors that are emerging throughout today's reshaped enterprises in order to detect problems and avoid the risk of ransomware proliferating through business networks. KPMG's cyber professionals are working successfully with clients in a range of sectors to combat today's threats. Here are some actions that we recommend businesses take now and going forward to help improve cyber security, cyber-risk management and cyber resilience:

Security actions for today

— Businesses, exchanges and banks should deploy blockchain analytics tools and AML controls adapted to managing today's specific cryptocurrency services and risks.

— Assess the potential impacts of system and data loss on your business and prepare a response action plan and test it.

— Update security-awareness training and resources for post-COVID working.

— Check identity, authentication and access to IT systems. Check Endpoint Detection and Response (EDR) capabilities and what you can log and monitor.

— Check your incident-response capability and backups and get hacked by an ethical hacker to fully test your response.

Security actions going forward

— Prioritize continuous development of defenses and counter measures to address risks as costly attacks evolve and proliferate. Banks face exposure as clients receive illegal currency related to ransom attacks.

— Assess all technology changes for potential errors and examine remote-work environments for new vulnerabilities. Examine how process changes or technology innovations may raise the risk of an 'insider threat.' Embed security into all IT delivery processes to help ensure that errors and vulnerabilities are addressed as early as possible.

— Run an exercise based on a scenario that will have the greatest impact on your organization. Implement a program of precise and comprehensive assessments that will regularly test your defenses and response capabilities against relevant threats and vectors.

— Understand exactly what the adoption and expansion of cloud services means regarding shared security responsibilities.

Responding wisely and proactively to the soaring threat of ransomware has become critical to business continuity and there is little time to waste for firms to enhance their defenses and response strategies as this costly and potentially destructive trend continues.

[8] Verizon 2020 Data Breach Investigations Report

Contacts:

Katherine Robins
Partner, Cyber Security, Management Consulting
KPMG Australia
E: krobins@kpmg.com.au

Julio Ferron
Senior Consultant,
Financial Services/KPMG EMA Virtual Assets Fincrime-Tech Coordinator
KPMG in Spain
E: jferron@kpmg.es

Alexander Klöpper
Financial Services — Regulatory & Compliance, RegTech & Crypto /KPMG EMA VirtualAssets Fincrime-Tech Coordinator
KPMG in Germany
E: jkloepper@kpmg.com

Saahil Chopra
Associate Director, Cyber Security, Management Consulting
KPMG Australia
E: schopra4@kpmg.com.au

Priyank Baveja
Director, Cyber Security, Management Consulting
KPMG Australia
E: pbaveja1@kpmg.com.au

home.kpmg/blockchainanalytics

Some or all of the services described herein may not be permissible for KPMG audit clients and their affiliates or related entities.

---

home.kpmg/socialmedia

Designed by Evalueserve.

Publication name: Blockchain analytics tools offer new ways to 'follow the money' in ransomware cases

Publication number: 137648-G

Publication date: August 2021