SAYARI

Uncovering Transnational Money Laundering Schemes: The Global Network of Wang Yunhe

EXECUTIVE SUMMARY

On 28 May 2024, the U.S. Department of Treasury's Office of Foreign Asset Control (OFAC) designated Chinese national Yunhe Wang (aka Wang Yunhe) and two co-conspirators for allegedly operating a malicious botnet scheme, enabling them to collect and sell backdoor access to more than 19 million internet protocol addresses in nearly 200 countries, facilitating cyber crimes including financial fraud, identity theft, and child exploitation.[1] [2] The IP addresses used in the botnet also facilitated the submission of tens of thousands of fraudulent applications related to the Coronavirus Aid, Relief, and Economic Security Act programs by its users, resulting in the loss of over $5.9 billion to the U.S. government.[3]

The indictment further alleges that as the primary administrator of the botnet, Wang received approximately $99 million in either cryptocurrency or fiat currency from the sales of the compromised IP addresses, which he used to purchase luxury assets and real estate properties in the United States, China, Singapore, Thailand, the United Arab Emirates, and St. Kitts and Nevis.

Although publicly available court records and U.S. sanctions documents detail the vast international network Wang used to carry out his scheme, Sayari Graph's interconnected global data and network mapping tools reveal additional information about Wang Yunhe's activities beyond what was detailed in the indictment and subsequent sanctions, facilitating a more complete analysis of his network.

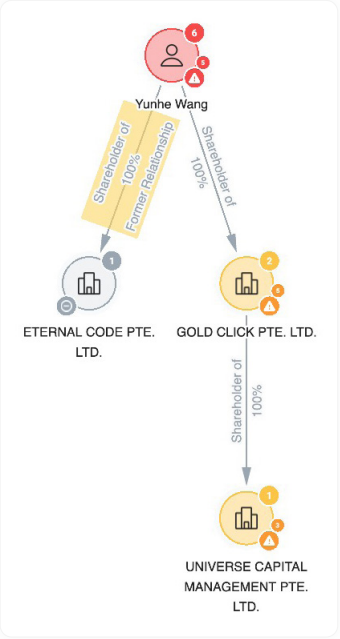
1 "Treasury Sanctions a Cybercrime Network Associated with the 911 S5 Botnet," U.S. Department of the Treasury: Press Releases (May 2024). https://home.treasury.gov/news/press-releases/jy2375

2 "United States of America v. Yunhe Wang," United States District Court for the Eastern District of Texas Sherman Division (May 2023). https://www.justice.gov/opa/media/1353516/dl?inline

3 "911 S5 Botnet Dismantled and Its Administrator Arrested in Coordinated International Operation," U.S. Department of Justice Office of Public Affairs: Press Releases (May 2024). https://www.justice.gov/opa/pr/911-s5-botnet-dismantled-and-its-administrator-arrested-coordinated-international-operation

Wang Yunhe's Corporate Network and Residence in Singapore

On 24 May 2024, Wang was arrested in Singapore, where he has continuously rejected extradition requests to the U.S.[4] Court documents identify his numerous connections to Singapore, including that he owned and operated a Singapore-incorporated company, Eternal Code, Pte. Ltd., and owned and resided in at least one property in Singapore. Given this footprint, it is not surprising that he is associated with multiple other companies also incorporated in Singapore, though they are not included in the public indictment or any related sanctions documents. While Eternal Code is no longer active in Singapore's national corporate registry, Wang is listed as the 100% shareholder of Gold Click, Pte. Ltd., a holding company which is the 100% shareholder of Universe Capital Management Pte. Ltd., a management consultancy company. Both companies are registered to Wang's identified Singaporean address and were active as of October 2024, but neither appear in the public indictment. Though Wang and his closest co-conspirators have been sanctioned and arrested, other facilitators could continue to use ill-gotten assets associated with these companies, presuming complicity in his scheme.



Additionally, although this Singapore-based Gold Click was not identified in public reporting, a UK-based company also named Gold Click Limited was identified in association with Wang in the indictment. The company was one of nearly 700 companies registered to "Rm 101, Maple House, 118 High Street Purley CR8 2AD" between 2006 and 2018, the overwhelming majority of which had Chinese shareholders and were compulsorily dissolved between 2017 and 2019.

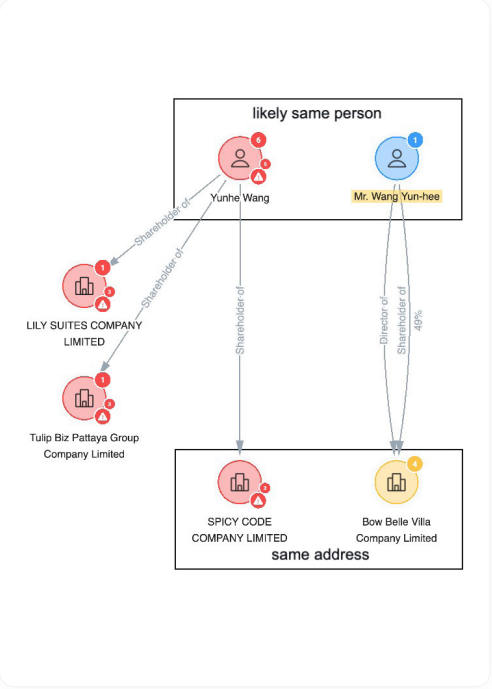
Sanctioned Real Estate Companies Reveal Additional Connections in Thailand

Obfuscation by Mistransliteration

In addition to Wang and his co-conspirators, OFAC sanctioned three Thai real estate companies for being owned and controlled by Wang, including Spicy Code Co., Ltd., Tulip Biz Pattaya Group Co., Ltd., and Lily Suites Co., Ltd.[5] An analysis of each of these companies' attributes in Sayari Graph reveals an additional company directly associated with Wang and numerous companies indirectly related through his sanctioned companies that have not previously been publicly identified.

4 Andrew Wong, "Man allegedly behind global malware network: Prosecution ready to present case for extradition to U.S.." Straits Times (June 2024). https://www.straitstimes.com/singapore/courts-crime/prosecution-ready-to-present-case-for-extradition-to-us-for-man-behind-global-malware-network

Thai corporate records reveal that Bow Belle Villa Co., Ltd. shares an address and real estate-related business purpose with the sanctioned Spicy Code and has a director and 49% shareholder "Wang Yun-hee," a very similar name to the sanctioned Wang Yunhe. Wang Yunhe appears in Thai corporate documents for his sanctioned companies as "นายหวัง หยุนเหอ," a phonetic translation of his Mandarin name pronounced "Wahng Yoon-huh." The Wang Yun-hee associated with Bow Belle Villa appears in Thai corporate documents as "นายหวัง ยุนฮ," a transliteration of a non-Thai name, possibly Mandarin given the parallels to Wang Yunhe. Notably, the Mandarin lexicon does not contain the sound "hee," increasing the likelihood that Wang Yun-hee is a misspelling or mistransliteration of Wang Yunhe. Like the indicted Wang Yunhe, the Wang Yunhee who appears in Thailand corporate record filings is a St. Kitts and Nevis citizen, increasing the odds that the indicted Wang Yunhe and the Thai-data Wang Yunhee are the same individual. If that is the case, Bow Belle Villa Co., Ltd. would be directly owned and controlled by Wang and should be sanctioned by operation of law along with Spicy Code, Tulip Biz Pattaya Group, and Lily Suites.



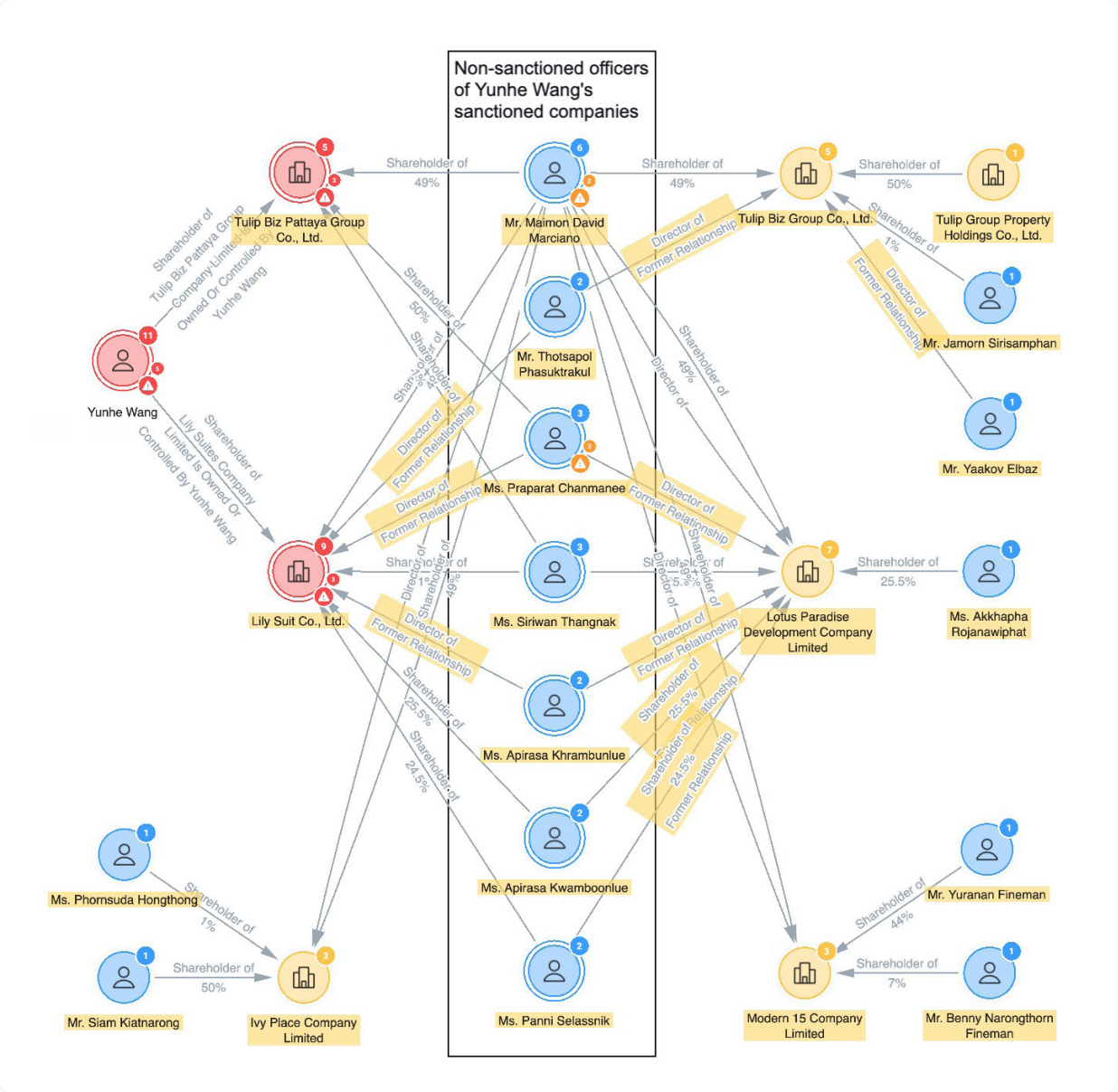
Connections via Potential Associates

Wang's other two sanctioned companies, Tulip Biz Pattaya Group and Lily Suites, report the same contact email: cmn_pattaya@hotmail.co.th. Querying this email in Sayari Graph reveals additional real estate companies with the same email, most of which match the same plant-themed naming convention and were incorporated in a similar time period. The companies disclosing this email address are as follows:

Company Name	Incorporation Date
Tulip Biz Group Co., Ltd.	16 June 2011
Tulip Biz Pattaya Group Co., Ltd. [SDN]	13 June 2012
Ivy Place Co., Ltd.	27 July 2012
Lily Suites Co., Ltd. [SDN]	30 July 2012
Lotus Paradise Development Co., Ltd.	30 July 2012
Modern 15 Company Limited	18 January 2017

5 Treasury: Press Releases (May 2024).

Most notably, all of these companies currently or formerly share multiple shareholders and directors with Tulip Biz Pattaya Group and Lily Suites, including 49% shareholder and director Maimon David Marciano. Maimon David Marciano has been a Pattaya condominium and hotel real estate developer since at least 2011, so connections to additional real estate companies aren't unexpected, but given the similar periods these companies were registered, further investigation into Marciano could potentially identify other companies involved in or which have benefited financially from Wang's scheme.[6] [7]



6 Pattaya People Media Group. 2021. "DAVID MARCIANO - GENEROU.S. MAN." March 17, 2021. https://www.facebook.com/PattayaPeople/posts/david-marciano-generous-mankhun-rattanachai-suthidechanai-was-representing- pat-ta/5271224739586214/

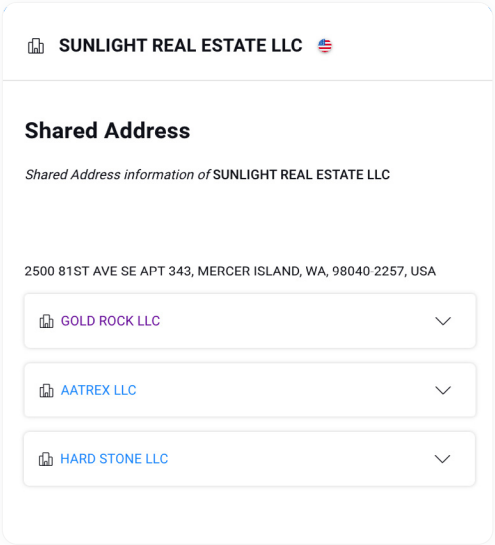
7 "Thailand's largest hotel chain and Pattaya developer join forces." Pattaya Mail (July 2011). https://www.pattayamail.com/business/thailands-largest-hotel-chain-and-pattaya-developer-join-forces-4947

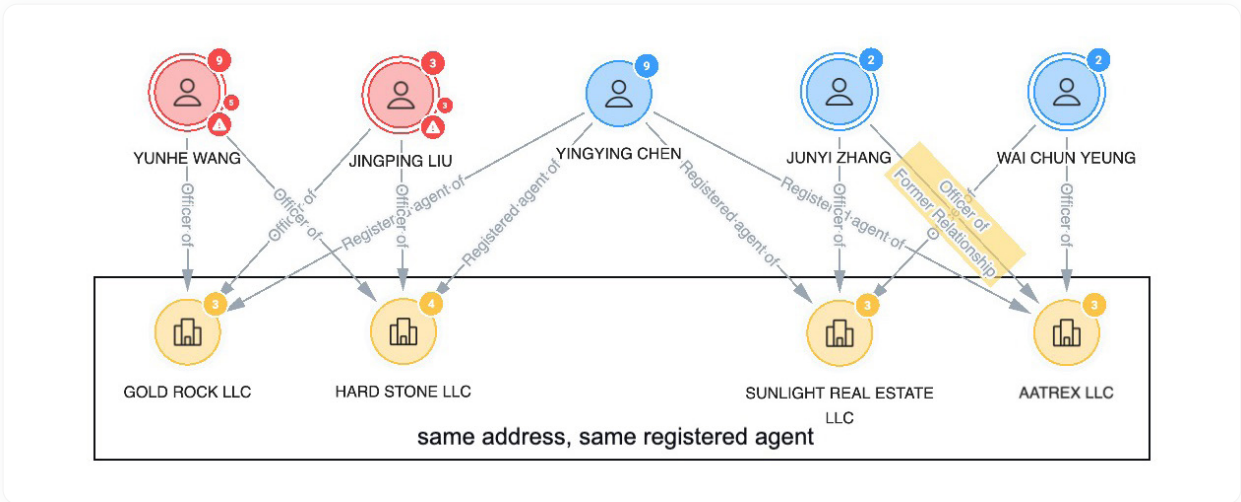
Co-Location Analysis in the U.S.

In addition to a presence in Thailand and Singapore, court documents also named two Washington, U.S.-based companies associated with Wang: Gold Rock LLC and Hard Stone LLC. Washington corporate documents reveal that Wang and his named co-conspirator Jingping Liu are listed as officers of the companies with registered agent Yingying Chen, who has not been named in relation to the case. Chen is the registered agent of seven other companies in Washington, likely the CPA or accountant according to his listed contact emails disclosed in corporate filings: yingying@u-needaccounting.com and chenyy.cpa@gmail.com. As the CPA, Chen would have direct access to Gold Rock and Hard Stone's business activities.

Two other companies associated with Chen – Sunlight Real Estate LLC and Aatrex LLC – are connected to Wang and his U.S. network. These two companies share an address with Wang's Washington-based companies and share officers Wai Chun Yeung and Junyi Zhang. Additionally, Wang's established use of real estate companies seen in his Thai network makes Sunlight Real Estate a potential funnel for his illicit earnings.

While Chen, Yeung, Zhang, and their associated companies have not been identified in public reporting, co-location and link analysis draws a compelling picture of Wang's network in the U.S.. Sharing an address, a registered agent, and a business purpose with multiple of Wang's known associated companies indicates that these companies could be facilitators of his network beyond what has currently been publicly identified in this case.

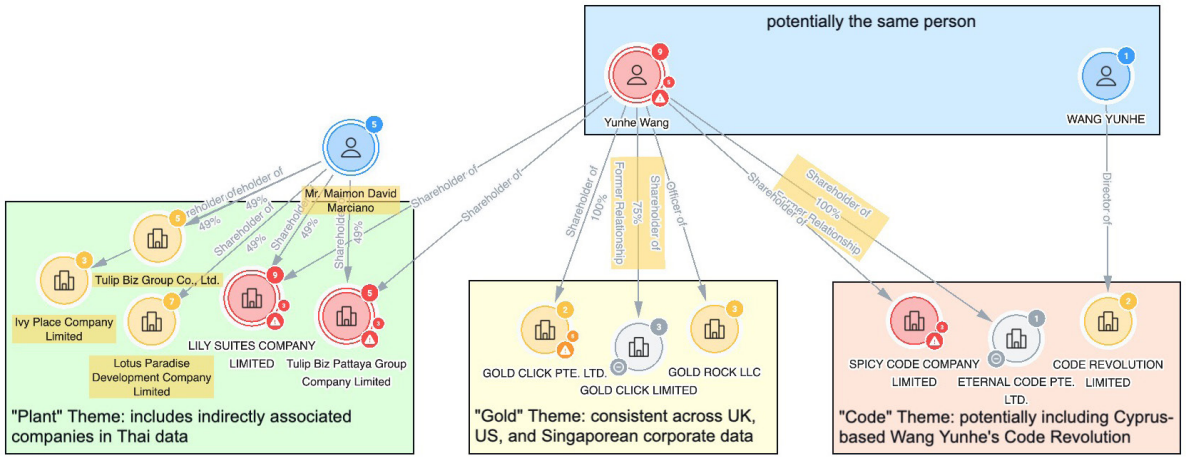




Wang Yunhe's Use of Secrecy Jurisdictions

Wang's network also reached several secrecy jurisdictions, including St. Kitts and Nevis, where he has citizenship by investment and owned an investment property, and the British Virgin Islands, where his company International Media Ltd. is based. International Media Ltd. owned the botnet software according to the botnet's End-User Licensing Agreement.[8] OFAC's sanctioning announcement and corresponding court documents confirmed these connections to opaque jurisdictions. Sayari Graph, however, also reveals a person named Yunhe Wang appearing in Cyprus, another well-known secrecy jurisdiction.

Secrecy jurisdictions notoriously report sparse information on their companies and the people behind them, so without access to original records, it is difficult to definitively conclude that this Cyprus-based Yunhe Wang is the same man sanctioned by OFAC. Despite this limitation, the naming convention suggests that the Cyprus-based Yunhe Wang and his company Code Revolution Ltd. could be connected to the sanctioned Yunhe Wang's companies Spicy Code and Eternal Code, as Wang tends to name and group companies thematically. For example, his Thai companies are named according to a "plant" theme and a "gold" theme appears across several jurisdictions, including Singapore-based Gold Click, UK-based Gold Click, and U.S.-based Gold Rock. The common name and similar company names cannot definitively link this Cyprus-based Wang to the sanctioned Wang's wider network, but merit additional research beyond the scope of this case study.



8 "A Deep Dive Into the Residential Proxy Service '911'," KrebsonSecurity (2022). https://krebsonsecurity.com/2022/07/a-deep-dive-into-the-residential-proxy-service-911/

Conclusion

In one of the largest fraud cases in recent history, Wang's money laundering scheme spans the globe, as established in unsealed court documents, public reporting, and augmented through public records link analysis in Sayari Graph. Using Graph to analyze public records associated with Wang, his co-conspirators, and his companies revealed additional people and companies possibly serving as unknown extensions of his network abroad. Co-location, contact information, network analysis, and pattern analysis using Graph uncovered additional leads across Singapore, Thailand, the United States, and Cyprus, revealing vectors through which Wang may have conducted his malware botnet, fraud, and real estate money laundering schemes.

ABOUT SAYARI

Sayari is the counterparty and supply chain risk intelligence provider trusted by government agencies, multinational corporations, and financial institutions. Its intuitive network analysis platform surfaces hidden risk through integrated corporate ownership, supply chain, trade transaction and risk intelligence data from over 250 jurisdictions.

Sayari is headquartered in Washington, D.C., and its solutions are used by thousands of frontline analysts in over 35 countries.

To learn how Sayari powers safer global commerce, please visit sayari.com. >