Ethereumの脆弱性と攻撃に関する調査

2020/09/25

横浜国立大学　吉岡克成

第2回BSEC研究会

Ethereumの脆弱性

- Ethereumクライアントの脆弱性
  - Go-Ethereum （Geth)の脆弱性[1]
  - JSON-RPCの設定不備[2]

- Ethereum スマートコントラクトの脆弱性[3]

[1] https://jvndb.jvn.jp/ja/contents/2018/JVNDB-2018-007680.html

[2] https://jp.cointelegraph.com/news/report-misconfigured-ethereum-clients-have-resulted-in-hack-of-around-20-mln

[3] Nicola Atzei, Massimo Bartoletti, and Tiziana Cimoli. A survey of attacks on ethereum smart contracts (sok). In International Conference on Principles of Security and Trust, pp. 164.186. Springer, 2017.

Ethereumの脆弱性

- **Ethereumクライアントの脆弱性**
  - **Go-Ethereum（Geth)の脆弱性[1]**
  - **JSON-RPCの設定不備[2]**

- Ethereum スマートコントラクトの脆弱性[3]

[1] https://jvndb.jvn.jp/ja/contents/2018/JVNDB-2018-007680.html

[2] https://jp.cointelegraph.com/news/report-misconfigured-ethereum-clients-have-resulted-in-hack-of-around-20-mln

[3] Nicola Atzei, Massimo Bartoletti, and Tiziana Cimoli. A survey of attacks on ethereum smart contracts (sok). In International Conference on Principles of Security and Trust, pp. 164.186. Springer, 2017.

Gethクライアントの脆弱な設定を突いた攻撃

Hackers Stole Over $20 Million From Misconfigured Ethereum Clients

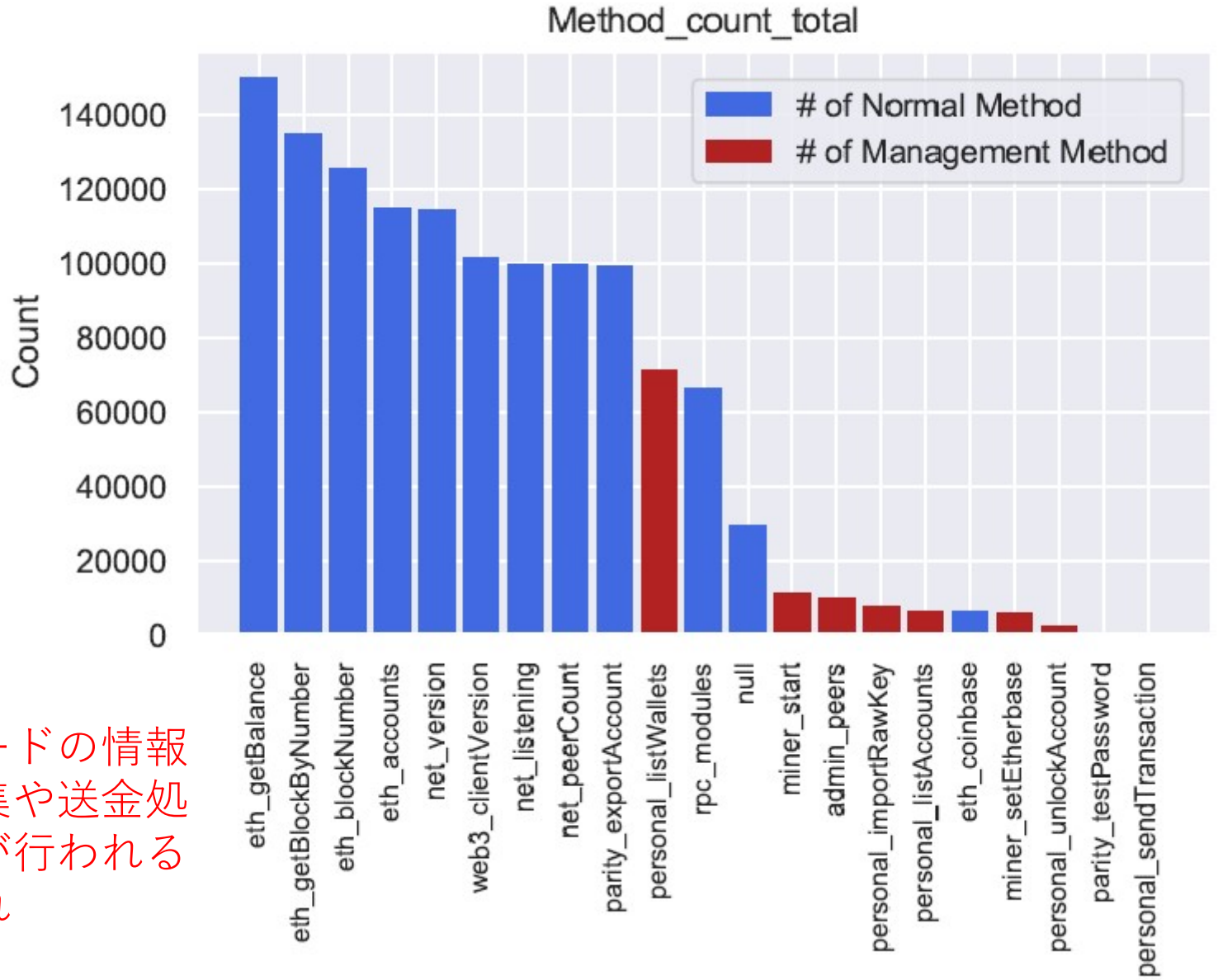
June 11, 2018

A group of hackers has stolen over $20 million worth of Ethereum from Ethereum-based apps and mining rigs, Chinese cyber-security firm Qihoo 360 Netlab reported today.

The cause of these thefts is Ethereum software applications that have been configured to expose an RPC [Remote Procedure Call] interface on port 8545.

https://www.bleepingcomputer.com/news/security/hackers-stole-over-20-million-from-misconfigured-ethereum-clients/

JSON-RPCエンドポイントの脆弱な設定を狙った攻撃(メソッド別)



ノードの情報収集や送金処理が行われる恐れ

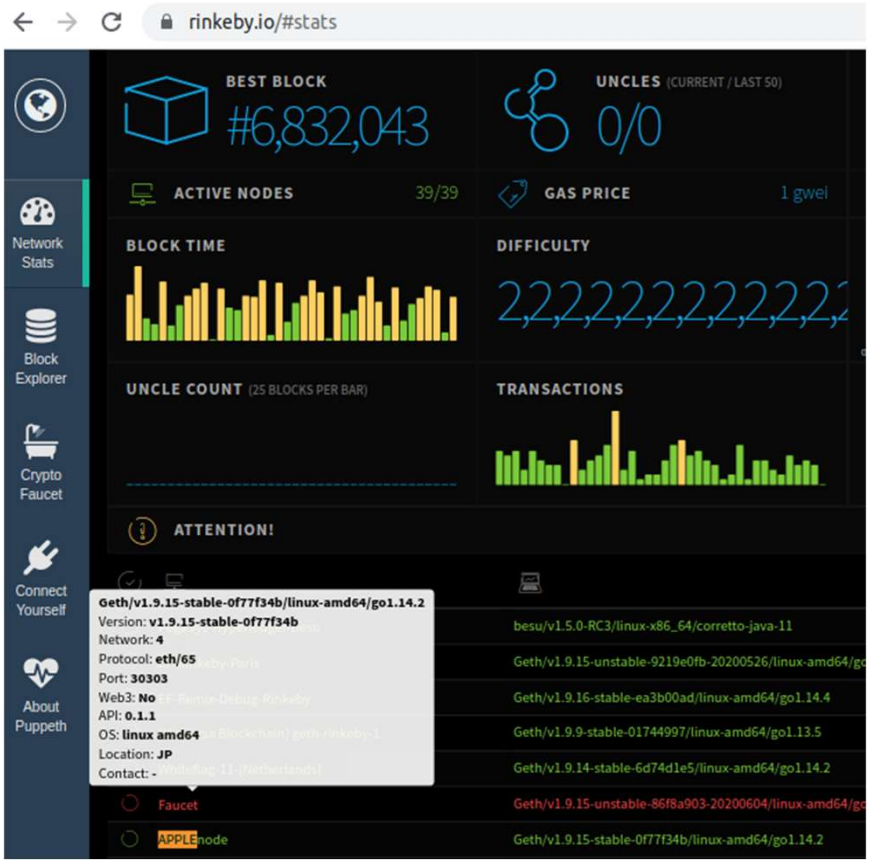
原　和希, 佐藤哲平, 今村光良, 面　和成, "ブロックチェーンネットワークにおけるハニーポット設置に向けた悪意あるユーザのプロファイリング," 電子情報通信学会情報セキュリティ研究会, 2019.

Honeypot with JSON-RPC Port Open

- Port 8545 opened on 20200702 with --rpc
  - Found port not open out of the machine
- Port 8545 opened globally on 20200709 –rpcaddr
  - Traffic capture restarted with daily spilt in tcpdump
- Port status began to show on Shodan from 20200713

Node Registration

- https://www.rinkeby.io/#stats
  - Both full and light nodes were registered on this website



Full Node named as “APPLEnode”

Light Node named as “PEARnode”

Port status on Shodan

114.156.141.196 p3665196-ipngnfx01hodogaya.kanagawa.ocn.ne.jp

cryptocurrency

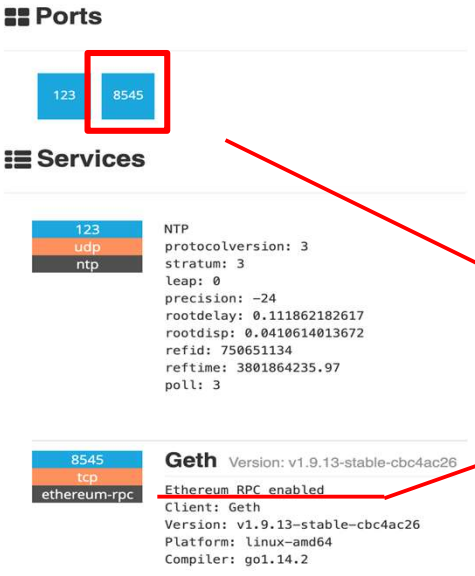
City	Setagaya-ku
Country	Japan
Organization	NTT
ISP	NTT
Last Update	2020-07-12T21:47:19.889220
Hostnames	p3665196-ipngnfx01hodogaya.kanagawa.ocn.ne.jp
ASN	AS4713

Full Node

222.229.219.133 static-222-229-219-133.b-man.svips.gol.ne.jp

cryptocurrency

City	Azabudai
Country	Japan
Organization	VECTANT
ISP	VECTANT
Last Update	2020-07-09T13:48:32.691665
Hostnames	static-222-229-219-133.b-man.svips.gol.ne.jp
ASN	AS2519

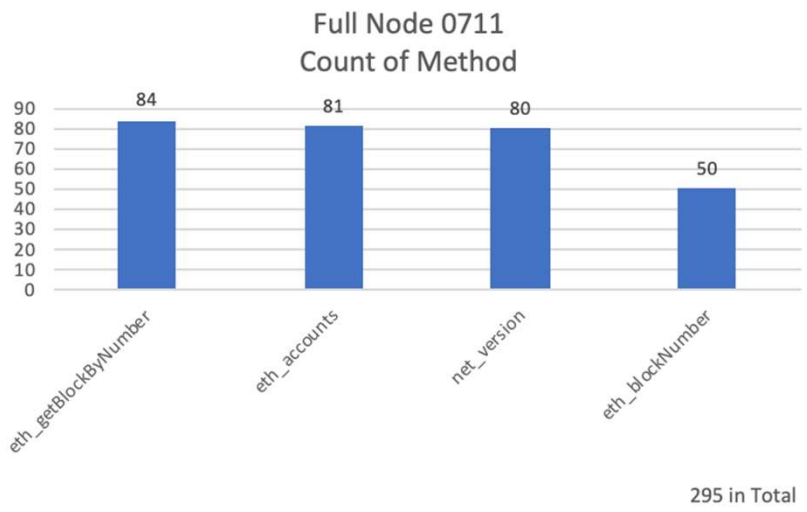


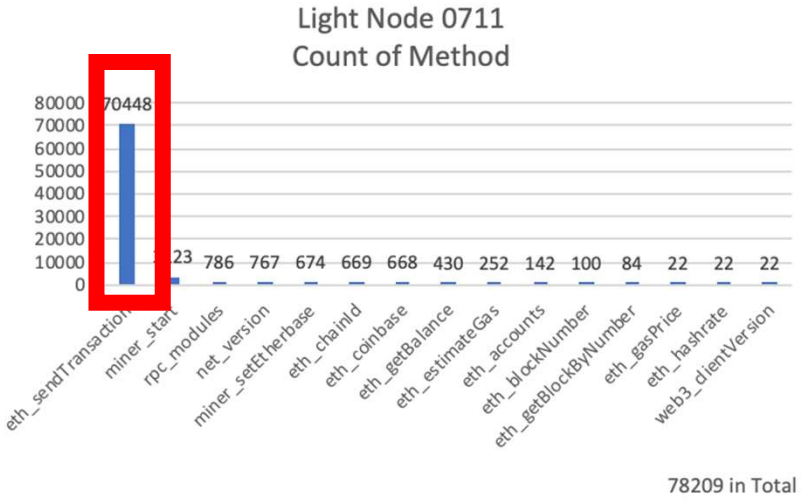
Light Node

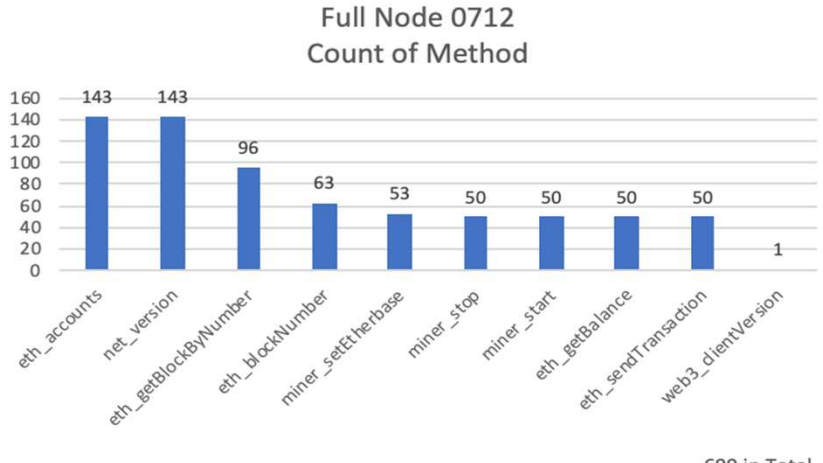
横浜国大Ethereumハニーポットで観測されたメソッド

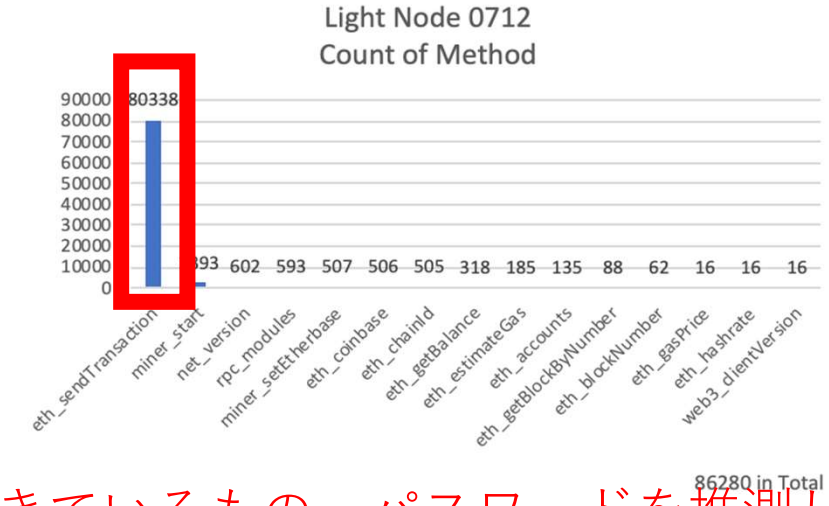
Method	Purpose	
miner_start	Start mining	Same
net_version	Get network version (tell apart mainnet and testnet)	
miner_setEtherbase	Specify the account to which obtained ether can be sent	
rpc_modules	Returns all enabled modules	
eth_getBalance	Get the balance of Ether	
eth_coinbase	Get the address of the node	
eth_accounts	Get the list of accounts	
eth_getBlockByNumber	Return information about a block by block number	
eth_blockNumber	Return the number of most recent block.	
web3_clientVersion	Return the current client (Geth) version	
eth_chainId	Get network version (tell apart mainnet and testnet)	New
eth_sendTransaction	Send transaction	
eth_estimateGas	Estimate of how much gas is necessary to allow the transaction to complete	
miner_stop	Stop mining	
eth_gasPrice	Return the current gas price in wei	
eth_hashrate	Return the number of hashes per second that the node is mining with	
eth_call	Another way to get token balance	
eth_getCode	Get the code of smart contract address	
net_listening		Not yet observed
net_peerCount		
parity_exportAccount		
personal_listWallets		
admin_peers		
personal_importRawKey		
personal_listAccounts		
persaonal_unlockAccount		
parity_tsetPassword		

Comparative Analysis By Daily









Eth_sendTransactionが大量に送られてきているもの、パスワードを推測して口座をアンロックし、送金を行うような挙動は観測されていない

Ethereumの脆弱性

- Ethereumクライアントの脆弱性
  - Go-Ethereum（Geth)の脆弱性[1]
  - JSON-RPCの設定不備[2]

- **Ethereum スマートコントラクトの脆弱性[3]**

[1] https://jvndb.jvn.jp/ja/contents/2018/JVNDB-2018-007680.html

[2] https://jp.cointelegraph.com/news/report-misconfigured-ethereum-clients-have-resulted-in-hack-of-around-20-mln

[3] Nicola Atzei, Massimo Bartoletti, and Tiziana Cimoli. A survey of attacks on ethereum smart contracts (sok). In International Conference on Principles of Security and Trust, pp. 164.186. Springer, 2017.

スマートコントラクト脆弱性の分類

Level	Cause of vulnerability
Solidity	Call to the unknown
	Gasless send
	Exception disorders
	Type casts
	Reentrancy
	Keeping secrets
EVM	Immutable bugs
	Ether lost in trasfer
	Stack size limit
Blockchain	Unpredictable state
	Generating randomness
	Time constraints

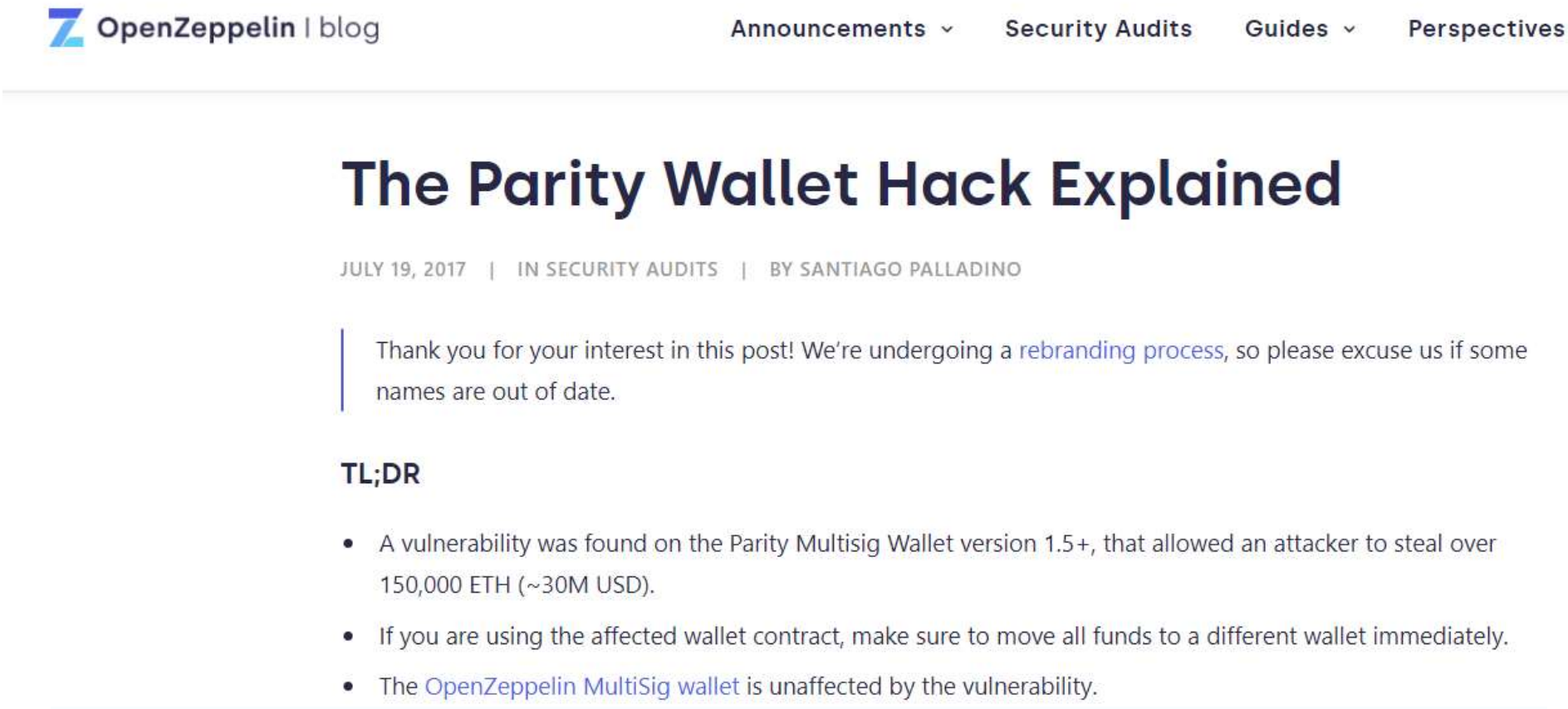
DAO attack(2016)

DAO attack(2016)

https://www.coindesk.com/understanding-dao-hack-journalists

Nicola Atzei, Massimo Bartoletti, and Tiziana Cimoli. A survey of attacks on ethereum smart contracts (sok). In International Conference on Principles of Security and Trust, pp. 164.186. Springer, 2017.

Parity Multisig Walletへの攻撃(2017)



https://blog.openzeppelin.com/on-the-parity-wallet-multisig-hack-405a8c12e8f7/

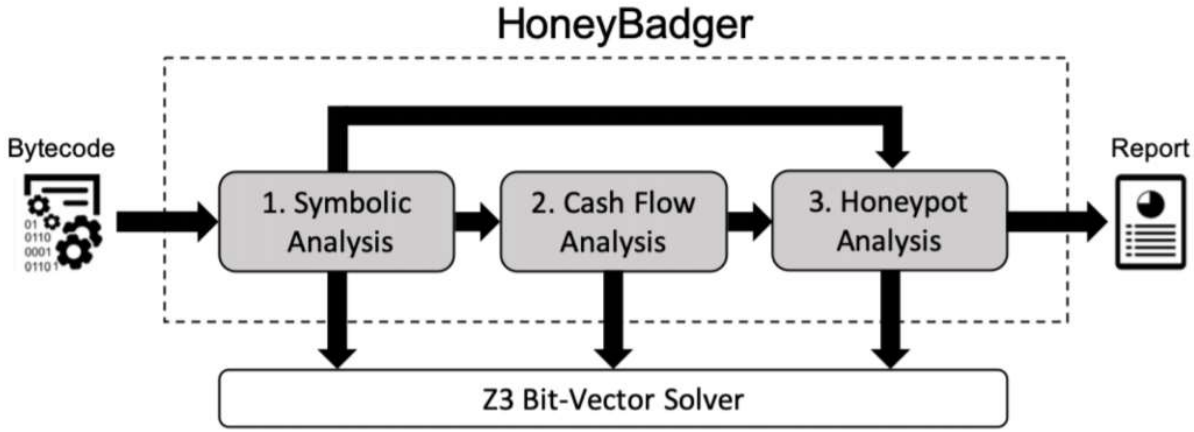
Ethereum Honeypot “Hacking the hacker”(2019)

“初心者”ハッカーを狙った
囮の脆弱コントラクト(悪意ハニーポット)の出現

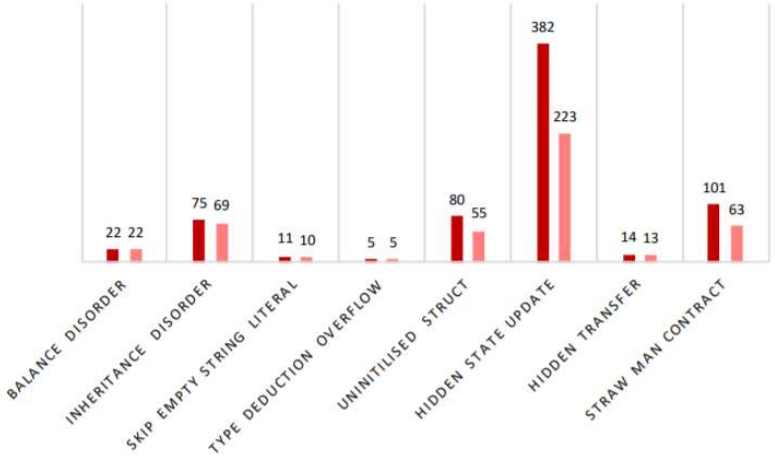
セキュリティ研究者のハニーポットではなく悪意のものである点に注意が必要

https://hackernoon.com/hacking-the-hackers-honeypots-on-ethereum-network-5baa35a13577

Ethereum Honeypot “Hacking the hacker”(2019)



- 48,487 contracts have been identified as cash flow contracts (32%).
- Our tool detected **460** unique honeypots (690 on the 2 million).
- Analysis took about 2 minutes per contract (91% code coverage).



２百万件のうち690件のコントラクトを悪意ハニーポットとして検出

Christof Ferreira Torres, Mathis Steichen and Radu State, "The Art of The Scam -Demystifying Honeypots in Ethereum Smart Contracts," USENIX SECURITY 2019.

実攻撃の観測研究(2020)

Incident	# contract	# tx	Loss	
			Direct (Ether / $)	Actual (Ether / $)
TheDAO	1	1,848	11,829,473 / $160,146,744	529,041 / $6,213,195
Parity Wallet Hack	622	2,710	204,851 / $40,700,890	154,999 / $31,009,177
SpankChain	1	8	165 / $37,321	165 / $37,321

* Note that although the actual ether loss of Parity Wallet Hack is less than the one of TheDAO, the monetary loss is higher due to the difference in historical ether price.

atx: adversarial transactions

Attacks	Known		Zero-day		Total Loss	
	# contract	# atx	# contract	# atx	ether / token	monetary
call injection	-	-	-	-	- / -	-
reentrancy	18	56	6	36	6,080 / 5.01E+23	$142,945
integer overflow	34	167	16	113	- / 7.79E+79	-
airdrop hunting	-	-	197	100,278	- / 3.59E+28	$322,010
call-after-destruct	154	1,547	74	214	472 / -	$100,102
honeypot	90	148	51	-	427 / -	$80,866
Total	285	1,904	344	100,641	6,979 / 7.79E+79	$645,848

Shunfan Zhou, Zhemin Yang, Jie Xiang, Yinzhi Cao, "Johns Hopkins University; Min Yang and Yuan Zhang, "An Ever-evolving Game: Evaluation of Real-world Attacks and Defenses in Ethereum Ecosystem," USENIX SECURITY 2020.

対策技術

最近数年間で、様々な方法でスマートコントラクトの脆弱性チェックを行う手法、ツールが提案・実装されている
トランザクションから攻撃を検知する手法もある

Tool	Inter-Contract	Memory	Keccak	Validation
Manticore [39]	◐	◐	◐	○
Mythril [41]	◐	◐	◐	○
MAIAN [46]	○	◐	◐	●
Oyente [36]	○	◐	○	○
teEther [33]	○	◐	◐	●
Vandal [4]	○	◐	○	○
MadMax [23]	○	◐	○	○
Securify [62]	○	◐	◐	○
ETHBMC	●	●	●	●

● Correctly implemented ◐ Partially implemented
○ Incorrectly implemented or missing

Joel Frank, Cornelius Aschermann, and Thorsten Holz, "EthBMC: A Bounded Model Checker for Smart Contracts," USENIX SECURITY 2020.

将来展望

- 脆弱性が存在するのは既存のプログラムもスマートコントラクトも同じ。脆弱性の発見やそれを突いた攻撃の検知など急速に研究が進んでいる。

- スマートコントラクトの脆弱性は、直接的な経済損失に繋がる意味で重要度が高い。

- 一方、ブロックチェーン上で発生しているため、攻撃やそれによる損失、対策活動が幅広く観測できる。また、過去にさかのぼって観測、分析、評価が出来る点、研究のためのデータ収集がしやすい点が、通常のサイバー攻撃の対策研究とは大きく異なる

→世界観が把握しやすく、データも収集しやすいのでAIの利用に向いている？
→現状、この性質は、対策側に有利に働いており、研究の進展を早めているように見えるが、攻撃側もこの性質を利用できる可能性はないか？

→逆に見えない部分では、どのような不正があり得るか？

最後に

- Ethereumの脆弱性についてクライアントソフトに起因するもの、スマートコントラクト自体に起因するものについてそれぞれ調査を行った結果を説明した。

- 特にスマートコントラクトの脆弱性や攻撃の検知、分析の研究が急速に進んでいる

- これらのセキュリティ技術がEthereumエコシステムのどの部分で利用され、どのようなエンティティがセキュリティ強化を進めるのか(例：セキュリティモニタリング，Audit serviceの展開など)、今後も動向を追いたい。
- システムセキュリティの観点での学術研究は、既に非常に競争が激しく、トップカンファレンスで多数の発表が行われているため、着目点を工夫しなければ、上位で戦うのは難しい印象。