

# Beosin: \$160 Million Lost in Wintermute's Exploit from Using Profanity



## Beosin: \$160 Million Lost in Wintermute's Exploit from Using Profanity

On Sep 20, 2022, Wintermute was exploited for about \$160M due to private key compromise. In June this year, Wintermute has already lost 20M Optimism (OP) tokens by an “internal mistake”. Beosin security team analyzed the incident and here’s what we found.

### 1. Incident Background

On Sep 20, 2022, Wintermute’s founder and CEO Evgeny Gaevoy tweeted that **Wintermute was hacked for about \$160M.**



**wishful cynic**  
@EvgenyGaevoy

...

We've been hacked for about \$160M in our defi operations. Cefi and OTC operations are not affected

4:03 PM · Sep 20, 2022 · Twitter Web App

303 Retweets 314 Quote Tweets 916 Likes



### Who can reply?

People @EvgenyGaevoy follows or mentioned can reply



**wishful cynic** @EvgenyGaevoy · 7h

...

Replying to @EvgenyGaevoy

We are solvent with twice over that amount in equity left

1

17

211



**wishful cynic** @EvgenyGaevoy · 7h

...

If you have a MM agreement with Wintermute, your funds are safe. There will be a disruption in our services today and potentially for next few days and will get back to normal after

1

17

173



Up to now, there are still a lot of addresses sending shitcoins or a small amount of Ether to the exploiter begging for some “relief”.

0xed81406eb899d63ad...	Transfer*	15579246	3 hrs 23 mins ago	0x1a7265dd3eae6d9509...	IN	Wintermute Exploiter	0 Ether	0.00023991
0x6911255f851d8762dbf...	Transfer*	15577345	9 hrs 46 mins ago	0xf30f9fdc881252e8c88...	IN	Wintermute Exploiter	1 wei	0.00038872
0x70168136b1a6d90138...	Transfer	15574635	18 hrs 52 mins ago	0x6e89fd0c96841cf6cce...	IN	Wintermute Exploiter	0 Ether	0.0003565
0x817bd302bdc0fd6c3b...	Transfer	15574306	19 hrs 59 mins ago	0xc821fcd1f88fb7ecb0e...	IN	Wintermute Exploiter	0 Ether	0.00011523
0x7b6130a920dbed4b70...	Transfer	15573937	21 hrs 14 mins ago	pag3t.eth	IN	Wintermute Exploiter	0.0001 Ether	0.00012316
0x0efad9aef8ea7730c6a...	Transfer	15573920	21 hrs 18 mins ago	0xe93be6a96579tc2772...	IN	Wintermute Exploiter	0.0001 Ether	0.00012406
0x1de06e9c7c5d585d64...	Transfer*	15573827	21 hrs 36 mins ago	Fake_Phishing6047	IN	Wintermute Exploiter	0 Ether	0.00017907
0x0426b7e89cf836e718...	Transfer*	15573813	21 hrs 39 mins ago	Fake_Phishing6047	IN	Wintermute Exploiter	0 Ether	0.00133517
0x9ee1fa1cd062749a4f...	Transfer*	15573780	21 hrs 46 mins ago	0xf30f9fdc881252e8c88...	IN	Wintermute Exploiter	1 wei	0.00017118
0x90ff30bba84c3b9a979...	Transfer*	15573779	21 hrs 46 mins ago	astronut.eth	IN	Wintermute Exploiter	0 Ether	0.00013453
0x3ee5f8c97d2654282a...	Transfer*	15573771	21 hrs 47 mins ago	0xfc928df037e99f05cdf3...	IN	Wintermute Exploiter	0 Ether	0.00011967
0x95cd19ab1f65358213...	Transfer*	15573771	21 hrs 47 mins ago	vae99.eth	IN	Wintermute Exploiter	0.0001 Ether	0.00013161
0x36fe7e77c9d054d90fb...	Transfer*	15573765	21 hrs 49 mins ago	astronut.eth	IN	Wintermute Exploiter	0 Ether	0.00011965

Value: 0 Ether (\$0.00)
Transaction Fee: 0.000119576549565792 Ether (\$0.16)

Gas Price: 0.000000005421497532 Ether (5.421497532 Gwei)
Ether Price: \$1,323.07 / ETH
Gas Limit & Usage by Txn: 33,084 | 22,056 (66.67%)
Gas Fees: Base: 3.921497532 Gwei | Max: 7.564040972 Gwei | Max Priority: 1.5 Gwei
Burnt & Txn Savings Fees: 🔥 Burnt: 0.000086492549565792 Ether (\$0.11) 💰 Txn Savings: 0.00004725593811264 Ether (\$0.06)

Others: Txn Type: 2 (EIP-1559) Nonce: 20 Position: 193

Input Data:

I haven't eaten for a few days, can you give me some money, thanks

View Input As

## 2. Incident Analysis

Attacker's address: 0xe74b28c2eae8679e3ccc3a94d5dode83ccb84705




























Attack contract: 0x0248f752802b2cfb4373ccoc3bc3964429385c26

Victim contract: 0x00000000ae34793obd1e7bof35588b9228of9e75

Beosin security team found that the attacker frequently used 0x0000000fe6a... address to call the 0x178979ae function of project's 0x00000000ae34... contract to transfer money to address 0x0248 (the attacker's contract).

TransactionsErc20 Token TxnsAnalyticsComments

IF Latest 25 from a total of 6,705 transactions

Txn Hash	Method	Block	Date Time (UTC)	From	To	Value	Txn Fee
 0x0d689ae5df735d40dc...	0x178979ae	15572702	2022-09-20 5:46:59	0x00000000fe6a514a32a...	 0x00000000ae347930bd...	0 Ether	0.00058178 
 0xefd8948379e2295184f...	0x178979ae	15572702	2022-09-20 5:46:59	0x00000000fe6a514a32a...	 0x00000000ae347930bd...	0 Ether	0.00054715 
 0x948fb49d7783a78bc8...	0x178979ae	15572702	2022-09-20 5:46:59	0x00000000fe6a514a32a...	 0x00000000ae347930bd...	0 Ether	0.00119107 
 0x8b9f4d4a86902eb1e4...	0x178979ae	15572702	2022-09-20 5:46:59	0x00000000fe6a514a32a...	 0x00000000ae347930bd...	0 Ether	0.00058447 
 0x9d349d3742ad50a41a...	0x178979ae	15572702	2022-09-20 5:46:59	0x00000000fe6a514a32a...	 0x00000000ae347930bd...	0 Ether	0.0005675 
 0xfce84987420e1da4a5...	0x178979ae	15572702	2022-09-20 5:46:59	0x00000000fe6a514a32a...	 0x00000000ae347930bd...	0 Ether	0.00061704 
 0x667559ba29645a6115...	0x178979ae	15572702	2022-09-20 5:46:59	0x00000000fe6a514a32a...	 0x00000000ae347930bd...	0 Ether	0.00057754 
 0x5caa93f73982772aef...	0x178979ae	15572702	2022-09-20 5:46:59	0x00000000fe6a514a32a...	 0x00000000ae347930bd...	0 Ether	0.00059178 
 0x3fa1955e9ae94a4153...	0x178979ae	15572702	2022-09-20 5:46:59	0x00000000fe6a514a32a...	 0x00000000ae347930bd...	0 Ether	0.00059187 

The project's contract is not open source. By decompiling the contract, we found that calling the 0x178979ae function requires permission checks.

```

271 function 0x178979ae(uint256 var0, uint256 var1, uint256 var2) public nonPayable {
272     require(msg.data.length - 4 >= 0x5);
273     require(var0 == address(var0));
274     require(var2 <= 0xffffffffffffffff);
275     require(4 + var2 + 31 < msg.data.length);
276     require(var2.length <= 0xffffffffffffffff, 65);
277     v0 = new bytes[(var2.length)];
278     require(!((v0 + (0xffffffffffffffffffffffffffffffffffffffff & (var2.length + 31 & 0xfffffffffffffffffffffffffffffffffffffee) + 32 + 31) < v0)
279     require(4 + var2 + var2.length + 32 <= msg.data.length);
280     CALLDATACOPY(v0.data, 4 + var2 + 32, var2.length);
281     v0[var2.length] = 0;
282     if (0xff & setCommonAdmin(msg.sender)) {
283         if (0xff & map_1[address(var0)]) {
284             if (stor_0 != 2) {
285                 stor_0 = 2;
286                 require(var1 <= this.balance, 0x3300000000000000000000000000000000000000000000000000000000000000);
287                 v1 = v2 = 0;
288                 while (v1 < v0.length) {
289                     MEM[v1 + v3.data] = v0[v1];
290                     v1 += 32;
291                 }
292                 if (v1 > v0.length) {
293                     MEM[v3.data + v0.length] = 0;
294                 }
295                 v4, v5, v6 = address(var0).call(v3.data).value(var1).gas(msg.gas);
296                 if (RETURNDATASIZE() != 0) {
297                     v7 = v8 = new bytes[(RETURNDATASIZE())];
298                     RETURNDATACOPY(v8.data, 0, RETURNDATASIZE());
299                 }
300                 if (lv4) {
301                     emit 0xd1a36f1ddcf3f4865169f66167a85ce8e4c1c1ba7217f402461495de7494476();
302                     goto 0x10a0;
303                 }
304                 stor_0 = 1;
305                 exit;

```

From the above source code we can see that 0x00000000fe6a address has Admin permission, so we deploy an contract to call setCommonAdmin() function for permission query, and we confirm that 0x00000000fe6a address has setCommonAdmin permission. The address has normal interaction with the contract before the attack, then we can confirm that 0x00000000fe6a's private key is compromised.

Combined with the address characteristics (0x00000000), it is suspected that the project used the Profanity tool to generate the address. The tool has been reported with a risk of brute force cracking of the private key in a previous article by researcher.



Wintermute's founder then confirmed on Twitter that Wintermute did use Profanity to generate addresses in June.

On September 15, [a report released by 1inch Network](#) claimed that Profanity is at the risk of brute force. The Profanity tool uses a 32-bit random vector to generate a 256-bit private key, which may be a security risk in this way.

First, the algorithm of the tool to generate the private key is:

- 1) Profanity will randomly select a 32-bit seed private key in the key space of  $2^{32} = 4294967296$ .
- 2) It is then expanded to 2 million private keys using some deterministic key expansion algorithm.
- 3) Calculate the corresponding derived public key based on the derived private key.
- (4) Repeatedly "increment" the derived public key until the corresponding vanity address is calculated.

Note: The "increment" mentioned in the blog, most people think that if the address derived from the public key in the algorithm does not meet the conditions for a vanity number, each derived private key will be added by 1 and the calculation of steps 2–4 will be repeated.

Secondly, the blogpost mentions a brute-force cracking method to get the initial key.

- 1) Calculate all the key spaces in advance, i.e. the public keys corresponding to the 4294967296 private keys, and store them in the hash table.



2) Obtain the transaction signature from the blockchain explorer and recover the public key from the transaction signature R, S, V values.

(3) Also extend the public key to 2 million public keys using deterministic key extension algorithm.

(4) Repeatedly “decrement” the derived public key until the seed public key is obtained.

5) Find out the corresponding private key in the hash table according to the seed public key.

Note: Similarly, the “decrement” here, most people think that if the derived public key obtained in the algorithm is different from the seed public key stored in the hash table, then each public key will be decremented by 1 and the operation will be repeated in 3–4 steps.

So many people have some questions about this way mentioned in the blog. First of all, in the private key extension algorithm, since the private key is calculated using secp256k1 elliptic curve algorithm to calculate the public key, the operation is not linear making the public key obtained from two private keys with a value difference of 1 also have a very big difference. Therefore, the same extension algorithm cannot be used to extend the public key in theory.

Second, also due to the elliptic curve algorithm itself, when the private key takes the operation of adding 1 for the iterative calculation of the public key, the inverse operation of adding 1 for the public key, i.e., the operation of subtracting 1, which also cannot effectively improve the calculation speed.

The dev himself answered the above query. The Profanity tool key extension algorithm uses the formula:

$$\text{privateKey} + (\text{task\_id} \ll 192)$$

Therefore the algorithm has an inverse operation:

$$\text{publicKey} - (\text{task\_id} \ll 192) * G$$

Also, since the key calculation is performed on a finite field, the corresponding “decrement” operation in the report is not a minus 1 operation, but a minus G point.

In summary, there are two problems with the Profanity tool. **Firstly, the key space is only 4 billion, which reduces the cost of blasting with the large amount of arithmetic power idle after the Ethereum merge. Secondly, the key expansion algorithm has the problem of inverse operations.**

### 3. Fund Flow

#### Fund source

The attacker's funding source was the 10 ETH withdrawn from Tornado Cash 1 day before the attack.

Transactions	Internal Txns	Erc20 Token Txns	Erc721 Token Txns	Erc1155 Token Txns	Analytics	Comments
Latest 2 Internal transactions						
Parent Txn Hash	Block	Age	From	To	Value	
0x16e49e81bf79862c91...	15572675	1 day 1 hr ago	Wrapped Ether	Wintermute Exploiter	6,919.69254349 Ether	
0x46eec2398ce207ee11...	15572374	1 day 2 hrs ago	Tornado.Cash: 10 ETH	Wintermute Exploiter	9.9435 Ether	

#### Stolen funds breakdown

attack address	TokenSymbol	value	Total stolen funds
1b28c2eae8079e3ccc3a94d5d0de83ccb8	WETH	6,919.69	\$159,417,832.71
	DAI	11,026,503.12	
	USDC	61,350,986.34	
	USDT	29,461,553.77	
	TUSD	3,246,604.78	
	BUSD	9,470,755.92	
	USDP	3,972,017.93	
	WETC	671.25	
	CUBE	1,789,602.46	
	MPL	59,407.37	
	eXRD	14,160,166.98	
	SNX	261,186.40	
	FTX Token	26,852.69	
	MATIC	820,956.78	
	PRIMATE	30,248,063.86	
	QNT	5,222.57	
	MULTI	113,669.18	
	ROUTE	179,246.00	
	YGG	2,174,469.13	
	CRV	1,019,428.38	
	PLA	1,393,842.96	
	NYM	1,673,197.78	
	LCX	8,495,859.49	
	APE	80,966.18	
	REQ	4,922,375.39	
	RADAR	39,463,145.11	
	SHIB	65,563,711,793.06	
	LDO	408,281.12	
	AAVE	4,617.16	
	SUSHI	279,275.83	
	GODS	701,554.43	
	DYDX	429,795.70	
	DPI	7,009.58	
	1INCH	414,495.78	
	ELON	1,127,528,944,057.05	
	CUDOS	36,276,385.41	
	ALI	15,914,254.19	
	ERN	218,005.75	
	FTM	871,944.63	
	CTX	63,500.51	
	ANGLE	4,647,645.54	
	NEXO	203,574.00	
	RAD	82,110.43	
	LOOT	388,208.78	
	GRT	2,827,278.56	
	PUSH	609,149.68	
	LON	268,842.68	
	COMP	3,283.18	
	INX	298,149.40	
	SAND	177,452.43	
	UNI	26,720.31	
	OMG	74,846.71	
	ZRX	417,169.67	
	MANA	204,829.52	
	LINK	13,897.07	
	KP3R	930.28	
	CRO	848,288.37	
	INDEX	36,857.36	
	SRM	115,749.74	
	YFI	10.08	
	SD	226,615.86	
	PSP	3,197,983.06	
	BOND	13,952.08	
	REVV	4,211,473.00	
	AMP	12,566,172.58	
	RLC	51,745.51	
	SKL	1,527,865.40	
	REN	547,177.29	
	BAT	74,550.76	
	BAND	40,313.51	
	RNDR	79,088.59	
	GALA	792,368.10	
	LRC	99,448.28	
	AUDIO	117,661.52	
	MKR	282.48	



According to Beosin Trace statistics, 75 types of assets are involved in the stolen funds, with a total value of about \$160 million. About 110 million of DAI/USDC/USDT were deposited into the Curve.fi protocol, gaining 110 million LP tokens, ranking the #3 holder in the 3Crv pool.

Transfers	Holders	Info	DEX Trades	Contract	Analytics	Comments
Token Holders Chart						
Top 1,000 holders (From a total of 8,089 holders)						
First < Page 1 of 20 > Last						
Rank	Address	Quantity	Percentage	Analytics		
1	Frax Finance: FRAX3CRV-f Token	238,003,110.740263277755998814	28.0104%			
2	Curve.fi: DAI/USDC/USDT Gauge	137,520,023.467540985649950145	16.1846%			
3	Wintermute Exploiter	111,953,508.959916301101032331	13.1757%			
4	0xed279fdd11ca84beef15af5d39bb4d4bee23f0ca	52,891,266.719222244184524955	6.2247%			
5	Curve.fi: aiUSD Factory Pool	49,680,917.955515148048405754	5.8469%			
6	0xeccd5e75afb02efa118af914515d6521aabd189f1	48,310,185.900545217124770673	5.6856%			

All the stolen funds are currently held at the attacker's address.

In response to this incident, Beosin security team recommends that:

1. Wintermute needs to remove administrative privileges such as setCommonAdmin/owner for ox0000000fe6a address and other vanity addresses, and replace them with secure wallet addresses.
2. Other projects or users who use Profanity tool to generate vanity addresses should transfer assets ASAP.

## Contact

If you have need any blockchain security services, please contact us:

**[Website](#) [Email](#) [Official Twitter](#) [Alert](#) [Telegram](#) [LinkedIn](#)**