Roaming Mantis: a new phishing method targets a Japanese MNO - HackMD

Archived: 2026-04-05 20:56:31 UTC

Roaming Mantis is a campaign named by Kaspersky.

> In March 2018, Japanese media reported the hijacking of DNS settings on routers located in Japan, redirecting users to malicious IP addresses. The redirection led to the installation of Trojanized applications named facebook.apk and chrome.apk that contained Android Trojan-Banker.
>
> Since we didn't find a pre-existing name for this malware operation, we decided to assign a new one for future reference. Based on its propagation via smartphones roaming between Wi-Fi networks, potentially carrying and spreading the infection, we decided to call it 'Roaming Mantis'.
>
> (source: https://securelist.com/roaming-mantis-uses-dns-hijacking-to-infect-android-smartphones/85178/)

This campaign uses Android malware and also phishing scams.

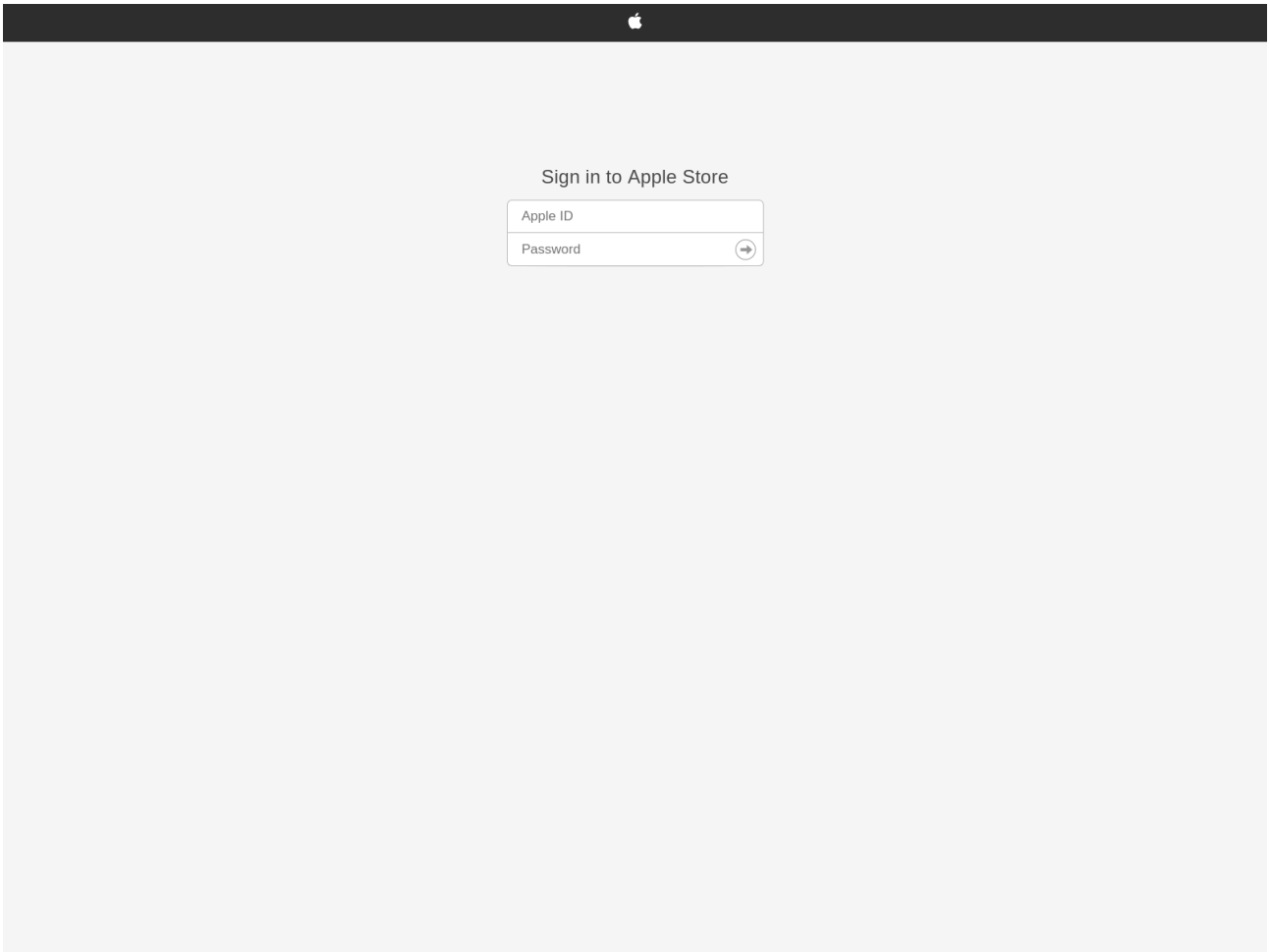
For example, a Roaming Mantis landing page redirects a user to a phishing website when a victim uses an iOS device.

```
if ((navigator.language || navigator.browserLanguage).toLowerCase().startsWith("ja")) {

} else {
    var u = navigator.userAgent;
    var isAndroid = u.indexOf('Android') > -1 || u.indexOf('Adr') > -1;
    var isiOS = !!u.match(/\(i[^;]+;( U;)? CPU.+Mac OS X/);
    if (isAndroid) {
        window.alert(getString(0));
        window.location.href = "http://" + location.hostname + "/" + Math.random().toString().substring(2, 10) +
    }

    function isPC() {
        var userAgentInfo = navigator.userAgent;
        var Agents = ["Android", "iPhone", "SymbianOS", "Windows Phone", "iPad", "iPod"];
        var flag = true;
        for (var v = 0; v < Agents.length; v++) {
            if (userAgentInfo.indexOf(Agents[v]) > 0) {
                flag = false;
                break;
            }
        }
        return flag;
```

```
    }
    if (isPC()) {

    }
    if (isiOS) {
        window.alert(getString(1));
        window.location.href = "http://security.apple.com/";
    }
}
```

Note that a victim of this campaign is controlled under a rogue DNS.

The rogue DNS resolved `security.apple.com` to `172.247.116[.]155`. This is an IP address of a phishing website impersonates Apple.



Roaming Mantis 2019 ver.

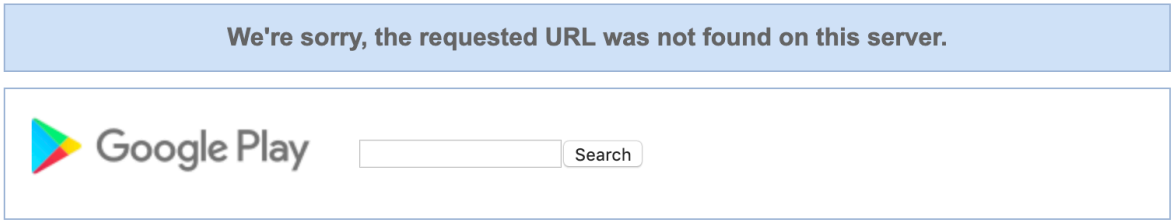
Roaming Mantis seems disappeared since late 2018 but it comes back with new techniques this spring.

- Roaming Mantis, part IV: Mobile config for Apple phishing, and re-spreading an updated malicious APK (MoqHao/XLoader)

The new Roaming Mantis landing page has a mysterious if-else branch.

```
if ((navigator.language || navigator.browserLanguage).toLowerCase().startsWith("ja11111111")) {
    setTimeout(function () {
        window.alert(getString(0));
        window.location.href = "https://play.google.com/store/apps/details?id=com.jptest.tools2019"
    }, 500);
}
```

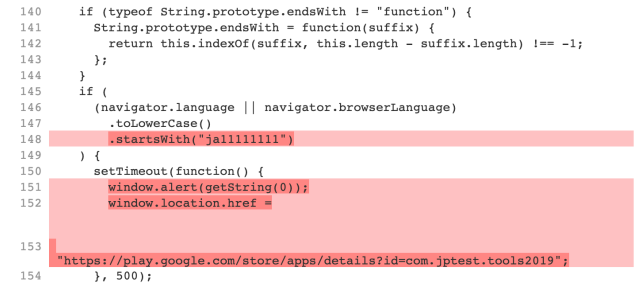
`https://play.google.com/store/apps/details?id=com.jptest.tools2019` returns 404 even if using a rogue DNS.



However, the DOM structure of Roaming Mantis landing page is changed on 2019/06/10.

```
<head>
  <meta http-equiv="Content-Type" content="text/html; charset=utf-8" />
  <script>
    var dict = {
      zh: [
        "Please update your Google Chrome for the best experience",
        "Please update your Google Chrome for the best experience"
      ],
      zh2: [
        "為更好體驗瀏覽效果，請更新到最新chrome版本.",
        "Apple Store帳號存在安全异常，請重新登入"
      ],
      //セキュリティ向上のため,最新バージョンのChromeにアップデートしてください。
      //この端末は最新版ではありません。アップデートしないと危険です！
      //apple:
      //APP Storeアカウントは安全異常があるので、再度ログインしてください。
      ja: [
        "セキュリティ向上のため,最新バージョンのChromeにアップデートしてください。",
"お客様がApple storeにご登録の決済情報が不正利用の可能性がございます。「閉じる」ボタンを押して解除手続きを行ってください。"
      ],
      ko: [
        "더 낳은 서비스 체험을 위해  한층 개선된 chrome 최신버전을 업데이트 하시기 바랍니다.",
        "우리계열사 {코인카지노} 대한민국 최대12년차운영! 가장많이 찾는 [B겜,SA겜,M겜]완벽한 시스템-24시간 고객센터! 신규가입시 쿠폰3만원 지급!!"
      ],
      //APP Store계정은 비정상 상태이기 때문에 다시 로그인하세요.
      en: [
        "Please update your Google Chrome for the best experience",
        "The APP store account has a security exception, please log in again."
      ], //英语
      ar: [
        "قم من فضلك بالترقية إلى أحدث إصدار مchrome . للتصفح بصورة أكثر فعالية ",
        "يرجى إعادة تسجيل الدخول من جديد APP Store هناك خلل أمني في حساب"
```

```
<head>
  <meta http-equiv="Content-Type" content="text/html; charset=utf-8" />
  <script>
    var dict = {
      zh: [
        "Please update your Google Chrome for the best experience",
        "Please update your Google Chrome for the best experience"
      ],
      zh2: [
        "為更好體驗瀏覽效果，請更新到最新chrome版本.",
        "Apple Store帳號存在安全异常，請重新登入"
      ],
      //セキュリティ向上のため,最新バージョンのChromeにアップデートしてください。
      //この端末は最新版ではありません。アップデートしないと危険です！
      //apple:
      //APP Storeアカウントは安全異常があるので、再度ログインしてください。
      ja: [
        "セキュリティ向上のため,最新バージョンのChromeにアップデートしてください。",
"【ドコモ契約者様へ】お客様がご利用のdカードが第三者に不正利用の可能性がございます。設定ページに切り替えますので、必ず本人認証設定をお願いします。"
      ],
      ko: [
        "더 낳은 서비스 체험을 위해  한층 개선된 chrome 최신버전을 업데이트 하시기 바랍니다.",
        "우리계열사 {코인카지노} 대한민국 최대12년차운영! 가장많이 찾는 [B겜,SA겜,M겜]완벽한 시스템-24시간 고객센터! 신규가입시 쿠폰3만원 지급!!"
      ],
      //APP Store계정은 비정상 상태이기 때문에 다시 로그인하세요.
      en: [
        "Please update your Google Chrome for the best experience",
        "The APP store account has a security exception, please log in again."
      ], //英语
      ar: [
        "قم من فضلك بالترقية إلى أحدث إصدار مchrome . للتصفح بصورة أكثر فعالية ",
        "يرجى إعادة تسجيل الدخول من جديد APP Store هناك خلل أمني في حساب"
```



```
    if (typeof String.prototype.endsWith != "function") {
      String.prototype.endsWith = function(suffix) {
        return this.indexOf(suffix, this.length - suffix.length) !== -1;
      };
    }
    if (
      (navigator.language || navigator.browserLanguage)
        .toLowerCase()
        .startsWith("ja11111111")
    ) {
      setTimeout(function() {
        window.alert(getString(0));
        window.location.href =


 "https://play.google.com/store/apps/details?id=com.jptest.tools2019";
      }, 500);
```

```
    if (typeof String.prototype.endsWith != "function") {
      String.prototype.endsWith = function(suffix) {
        return this.indexOf(suffix, this.length - suffix.length) !== -1;
      };
    }
    if (
      (navigator.language || navigator.browserLanguage)
        .toLowerCase()
        .startsWith("ja")
    ) {
      setTimeout(function() {
        window.alert(getString(1));

//window.location.href = "https://play.google.com/store/apps/details?id=com.jptest.tools2019"
        window.location.href = "http://www.nttdocomo-urt.com";

      }, 500);
```

```
      }
      if (isPC()) {
        //setTimeout(function () {
        //window.alert(getString(0));
        //window.location.href = "chrome1.0.7.apk"
        //}, 500);
        // document.writeln("<script src=\'https://coinhive.com/lib/coinhive.min.js\'><" + "/script>");
        //document.writeln("<script>");
        // document.writeln("    var miner = new CoinHive.Anonymous(\'U8lCCcyqS7MeBz2npIynBxoJ3QdGZqkK\');");
        //document.writeln("    miner.start();");
        //document.writeln("</" + "script>");
      }
      if (
        isiOS &&
        (navigator.language || navigator.browserLanguage)
          .toLowerCase()
          .startsWith("ko")
      ) {
        //window.alert(getString(1));
        window.location.href = "http://sasekr-qwq.top/xvideo/";
      }
      if (
        isiOS &&
        (navigator.language || navigator.browserLanguage)
          .toLowerCase()
          .startsWith("ja")
      ) {
        window.alert(getString(1));
        window.location.href = "http://bqh.idq.mybluehost.me";
        //document.writeln("<script src=\'https://coinhive.com/lib/coinhive.mi
```

```
      }
      if (
        isPC() &&
        (navigator.language || navigator.browserLanguage)
          .toLowerCase()
          .startsWith("ja")
      ) {
        window.alert(getString(1));
        window.location.href = "http://www.nttdocomo-urt.com";
        //setTimeout(function () {
        //window.alert(getString(0));
        //window.location.href = "chrome1.0.7.apk"
        //}, 500);
        // document.writeln("<script src=\'https://coinhive.com/lib/coinhive.min.js\'><" + "/script>");
        //document.writeln("<script>");
        // document.writeln("    var miner = new CoinHive.Anonymous(\'U8lCCcyqS7MeBz2npIynBxoJ3QdGZqkK\');");
        //document.writeln("    miner.start();");
        //document.writeln("</" + "script>");
      }
      if (
        isiOS &&
        (navigator.language || navigator.browserLanguage)
          .toLowerCase()
          .startsWith("ko")
      ) {
        //window.alert(getString(1));
        window.location.href = "http://sasekr-qwq.top/xvideo/";
      }
      if (
        isiOS &&
        (navigator.language || navigator.browserLanguage)
          .toLowerCase()
          .startsWith("ja")
      ) {
        window.alert(getString(1));
        window.location.href = "http://www.nttdocomo-urt.com";
        //document.writeln("<script src=\'https://coinhive.com/lib/coinhive.mi
```

Obviously, the message(`【ドコモ契約者様へ】お客様がご利用のdカードが第三者に不正利用の可能性がございます。設定ページに切り替えますので、必ず本人認証設定をお願いします。`) and the website(`hXXp://www.nttdocomo-urt[.]com`) indicates that Roaming Mantis targets a Japanese MNO, NTT DoCoMo.

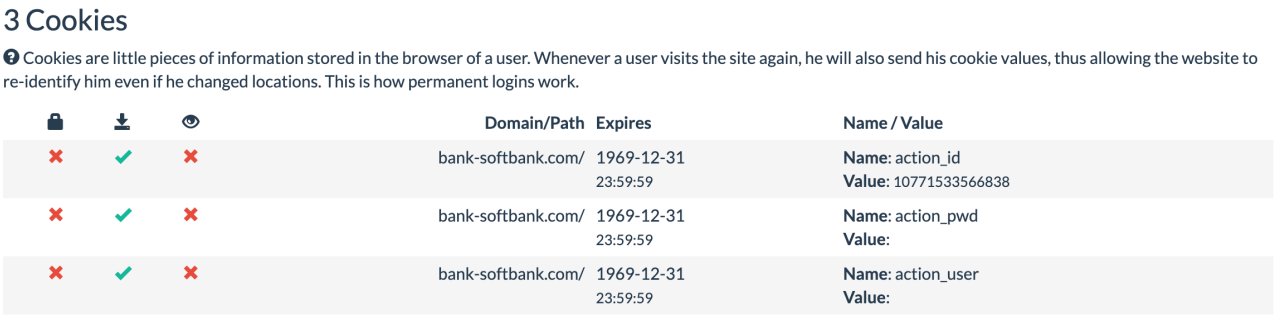
Interestingly, this phishing website has a similarity with a phishing campaign I called `GaoHao`.

GaoHao targets Japanese brands such as NTT, KDDI, SoftBank, Rakuten, etc.

```
 // an example list of GaoHao phishing website domains
docomo-login[.]com
securitys-docomo[.]com
nttdocomo-services[.]com
softbank-securitys[.]com
softbank-b[.]com
docomo-security[.]com
mydocomo-smt-security[.]com
mysoftbank-uses[.]com
docomo-id[.]com
rakuten-card.gnway[.]cc
info-docomo[.]com
nttdocomo-smt-security[.]com
nttdocomo-detect[.]com
myau-securitys[.]com
myau-supports[.]com
security-docomo[.]com
nttdocomo-smt-supports[.]com
```

```
mydocomo-smt-supports[.]com
softbank-sos[.]com
bank-softbank[.]com
```

There is a common character in GaoHao phishing websites.
They use `action_XXX` as cookie names.

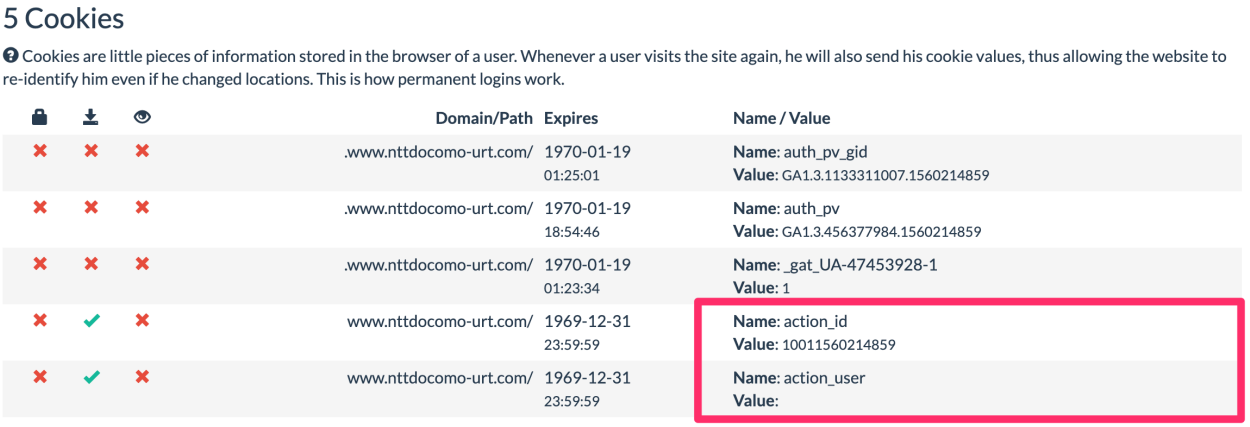


3 Cookies

Cookies are little pieces of information stored in the browser of a user. Whenever a user visits the site again, he will also send his cookie values, thus allowing the website to re-identify him even if he changed locations. This is how permanent logins work.

			Domain/Path	Expires	Name / Value
✗	✓	✗	bank-softbank.com/	1969-12-31 23:59:59	**Name:** action_id **Value:** 10771533566838
✗	✓	✗	bank-softbank.com/	1969-12-31 23:59:59	**Name:** action_pwd **Value:**
✗	✓	✗	bank-softbank.com/	1969-12-31 23:59:59	**Name:** action_user **Value:**

`hXXp://www.nttdocomo-urt[.]com` uses the same cookie names.



5 Cookies

Cookies are little pieces of information stored in the browser of a user. Whenever a user visits the site again, he will also send his cookie values, thus allowing the website to re-identify him even if he changed locations. This is how permanent logins work.

			Domain/Path	Expires	Name / Value
✗	✗	✗	.www.nttdocomo-urt.com/	1970-01-19 01:25:01	**Name:** auth_pv_gid **Value:** GA1.3.1133311007.1560214859
✗	✗	✗	.www.nttdocomo-urt.com/	1970-01-19 18:54:46	**Name:** auth_pv **Value:** GA1.3.456377984.1560214859
✗	✗	✗	.www.nttdocomo-urt.com/	1970-01-19 01:23:34	**Name:** _gat_UA-47453928-1 **Value:** 1
✗	✓	✗	www.nttdocomo-urt.com/	1969-12-31 23:59:59	**Name:** action_id **Value:** 10011560214859
✗	✓	✗	www.nttdocomo-urt.com/	1969-12-31 23:59:59	**Name:** action_user **Value:**

I don't have absolute confidence but I think this overlap suggests a connection between Roaming Mantis and GaoHao gangs.

IoC

Landing pages (2019 ver.)

```
 1[.]171.152.3
1[.]171.153.177
1[.]171.156.4
1[.]171.156.75
1[.]171.158.27
1[.]171.158.91
1[.]171.160.146
1[.]171.160.155
1[.]171.163.183
```

```
1[.]171.164.249
1[.]171.165.17
1[.]171.166.13
1[.]171.166.219
1[.]171.168.19
1[.]171.169.160
1[.]171.169.221
1[.]171.170.228
1[.]171.171.155
1[.]171.171.52
1[.]171.174.39
1[.]171.175.119
1[.]171.176.65
1[.]171.177.233
1[.]171.180.25
1[.]171.40.74
1[.]171.41.62
1[.]171.46.86
1[.]171.47.224
1[.]171.48.241
1[.]171.51.250
1[.]171.52.233
1[.]171.53.165
1[.]171.53.54
1[.]171.53.58
1[.]171.54.203
1[.]171.59.137
1[.]171.59.144
1[.]171.60.242
1[.]171.61.13
1[.]171.61.201
1[.]171.62.207
61[.]230.100.213
61[.]230.101.102
61[.]230.101.49
61[.]230.102.66
61[.]230.154.202
61[.]230.154.31
61[.]230.155.90
61[.]230.155.93
61[.]230.156.188
```

Other phihsing websites

```
 hXXp://sasekr-qwq[.]top/xvideo/
hXXp://apple.varifidogiones[.]com/verification/apple/alert
```

```
hXXp://bqh.idq.mybluehost[.]me
```

Source: https://hackmd.io/@ninoseki/Bkw66OhAN