

Spyware vendors use 0-days and n-days against popular platforms

 blog.google/threat-analysis-group/spyware-vendors-use-0-days-and-n-days-against-popular-platforms/

Clement Lecigne

March 29, 2023


Threat Analysis Group

Google's Threat Analysis Group (TAG) tracks actors involved in information operations (IO), government backed attacks and financially motivated abuse. For years, TAG has been tracking the activities of commercial spyware vendors to protect users. Today, we actively track more than 30 vendors with varying levels of sophistication and public exposure selling exploits or surveillance capabilities to government backed actors. These vendors are enabling the proliferation of dangerous hacking tools, arming governments that would not be able to develop these capabilities in-house. While use of surveillance technologies may be legal under national or international laws, they are often found to be used by governments to target dissidents, journalists, human rights workers and opposition party politicians.

In this blog, we're sharing details about two distinct campaigns we've recently discovered which used various 0-day exploits against Android, iOS and Chrome and were both limited and highly targeted. The 0-day exploits were used alongside n-day exploits and took advantage of the large time gap between the fix release and when it was fully deployed on end-user devices. Our findings underscore the extent to which commercial surveillance vendors have proliferated capabilities historically only used by governments with the technical expertise to develop and operationalize exploits.

Campaign #1 - Your missed parcel included 0-days (CVE-2022-42856; CVE-2022-4135)


In November 2022, TAG discovered exploit chains with 0-days affecting Android and iOS that were delivered via bit.ly links sent over SMS to users located in Italy, Malaysia and Kazakhstan. When clicked, the links redirected visitors to pages hosting exploits for either Android or iOS then redirected them to legitimate websites such as the page to track shipments for Italian-based shipment and logistics company BRT or a popular Malaysian news website.

 Image of a screenshot from one of the malicious websites
An example screenshot from one of the malicious websites

iOS Exploit Chain

The iOS exploit chain targeted versions prior to 15.1 and contained the following exploits, including one 0-day:

- [CVE-2022-42856](#), a WebKit remote code execution exploiting a type confusion issue within the JIT compiler (0-day at time of exploitation).
- The exploit used a PAC bypass technique which was fixed in March 2022 when Apple removed DYLD_INTERPOSE from WebKit. The exact same technique was used in Cytrox exploits as described by Citizenlab in their [blog](#) about Predator. The “make_bogus_transform” function is part of the PAC bypass and is present in both exploits.

 Extract from CitizenLab report mentioning the “make_bogus_transform” function
Extract from CitizenLab report mentioning the “make_bogus_transform” function

[CVE-2021-30900](#), a sandbox escape and privilege escalation bug in AGXAccelerator, fixed by Apple in 15.1. The bug was previously described in an [exploit](#) for oob_timestamp published on Github in 2020.

 screenshot of code

Description of CVE-2021-30900 on an exploit for oob_timestamp (CVE-2020-3837)

The final payload was a simple stager that pings back the GPS location of the device and gives the attacker the ability to install an .IPA file (iOS application archive) onto the affected device.

Android Exploit Chain

The Android exploit chain targeted users on phones with an ARM GPU running Chrome versions prior to 106. It consisted of three exploits, including one 0-day:

- [CVE-2022-3723](#), a type confusion vulnerability in Chrome, found by Avast in the wild and fixed in October 2022 in version 107.0.5304.87.
- [CVE-2022-4135](#), a Chrome GPU sandbox bypass only affecting Android (0-day at time of exploitation), fixed in November 2022. Sergei Glazunov from Project Zero helped analyze the exploit and wrote a root cause analysis for this bug.
- [CVE-2022-38181](#), a privilege escalation bug fixed by ARM in August 2022. It is unclear if attackers had an exploit for this vulnerability before it was reported to ARM.

It's worth noting users were redirected to Chrome using Intent Redirection if they were coming from a Samsung Internet Browser. In the past, we have seen attackers redirect users from Chrome to Samsung Internet Browser, similar to [CVE-2022-2856](#), but in this case the redirection occurred the other way. We were unable to obtain the final payload for this exploit chain.

When ARM released a fix for CVE-2022-38181, patches were not immediately incorporated by vendors, resulting in the bugs exploitation. This was recently highlighted by blog posts from [Project Zero](#) and [Github Security Lab](#).

Note, Pixel devices with the 2023-01-05 security update are protected against both exploit chains in this blog. Chrome users updated to at least version 108.0.5359 are also protected.

Related IOCs

- [https://cdn.cutlink\[.\]site/p/uu6ekt](https://cdn.cutlink[.]site/p/uu6ekt) - landing page
- [https://api.cutlink\[.\]site/api/s/N0NBL8/](https://api.cutlink[.]site/api/s/N0NBL8/) - Android exploit chain
- [https://api.cutlink\[.\]site/api/s/3PU970/](https://api.cutlink[.]site/api/s/3PU970/) - iOS exploit chain
- [https://imjustarandomsite.3utilities\[.\]com](https://imjustarandomsite.3utilities[.]com) - exploit delivery server

Campaign #2 - Complete exploit chain against Samsung Internet Browser (CVE-2022-4262; CVE-2023-0266)

In December 2022, TAG discovered a complete exploit chain consisting of multiple 0-days and n-days targeting the latest version of Samsung Internet Browser. The exploits were delivered in one-time links sent via SMS to devices located in the United Arab Emirates (UAE).

The link directed users to a landing page identical to the one TAG examined in the [Heliconia framework](#) developed by commercial spyware vendor Variston. The exploit chain ultimately delivered a fully featured Android spyware suite written in C++ that includes libraries for decrypting and capturing data from various chat and browser applications. The actor using the exploit chain to target UAE users may be a customer or partner of Variston, or otherwise working closely with the spyware vendor.

The exploit chain TAG recovered was delivered to the latest version of Samsung's Browser, which runs on Chromium 102 and does not include recent mitigations. If they had been in place, the attackers would have needed additional vulnerabilities to bypass the mitigations. The exploit chain consisted of multiple 0-days and n-days:

- [CVE-2022-4262](#), a type confusion vulnerability in Chrome fixed in December 2022 (0-day at time of exploitation) - similar to [CVE-2022-1134](#).
- [CVE-2022-3038](#), a sandbox escape in Chrome fixed in August 2022, in version 105 and [found](#) by Sergei Glazunov in June 2022.
- [CVE-2022-22706](#), a vulnerability in Mali GPU Kernel Driver [fixed](#) by ARM in January 2022 and marked as being used in the wild. At the time of delivery, the latest Samsung firmware had not included a fix for this vulnerability. This vulnerability grants the attacker system access.

- [CVE-2023-0266](#), a race condition vulnerability in the Linux kernel sound subsystem reachable from the system user and that gives the attacker kernel read and write access (0-day at time of exploitation).

The exploit chain also took advantage of multiple kernel information leak 0-days when exploiting CVE-2022-22706 and CVE-2023-0266. Google reported these vulnerabilities to ARM and Samsung. CVE-2023-26083 was reserved for the information leak in Mali.

Note, Samsung fixed CVE-2022-4262 and CVE-2022-3038 in Samsung's Browser after version 19.0.6 released at the end of December 2022.

Related IOCs

- [www.sufficeconfigure\[.\]com](#) - landing page and exploit delivery
- [www.anglesyen\[.\]org](#) - malware C2
- The following Android system properties might indicate signs of exploitation
 - `sys.brand.note`
 - `sys.brand.notes`
 - `sys.brand.doc`
- The following directory on the phone might indicate signs of infection
`/data/local/tmp/dropbox`

Protecting our users

To protect our users, Google has reported these vulnerabilities to the vendors. We would be remiss if we did not acknowledge the quick response and patching of these vulnerabilities by Google's Chrome, Pixel and Android teams, as well as by Apple. We would also like to acknowledge and thank the Amnesty Security Lab for their help uncovering the second campaign detailed in this blog.

These campaigns continue to underscore the importance of patching, as users wouldn't be impacted by these exploit chains if they were running a fully updated device. Intermediate mitigations like PAC, [V8 sandbox](#) and [MiraclePTR](#) have a real impact on exploit developers, as they would have needed additional bugs to bypass these mitigations.

Conclusion

These campaigns are a reminder that the commercial spyware industry continues to thrive. Even smaller surveillance vendors have access to 0-days, and vendors stockpiling and using 0-day vulnerabilities in secret pose a severe risk to the Internet. These campaigns may also indicate that exploits and techniques are being shared between surveillance vendors, enabling the proliferation of dangerous hacking tools. We remain committed to updating the community, and taking steps to protect users, as we uncover these campaigns.

POSTED IN:

[Threat Analysis Group](#)

Related stories

- [Threat Analysis Group](#)
[TAG Bulletin: Q1 2023](#)

[Threat Analysis Group shares their Q1 2023 bulletin.](#)

By [Shane Huntley](#)

[May 01, 2023](#)

- [Threat Analysis Group](#)
[Ukraine remains Russia's biggest cyber focus in 2023](#)

[Google's Threat Analysis Group shares first quarter cyber updates on the threat landscape from the war in Ukraine.](#)

By [Billy Leonard](#)

[Apr 19, 2023](#)

- [Threat Analysis Group](#)
[How we're protecting users from government-backed attacks from North Korea](#)

[Google's Threat Analysis Group shares information on ARCHIPELAGO as well as the work to stop government-backed attackers.](#)

By [Adam Weidemann](#)

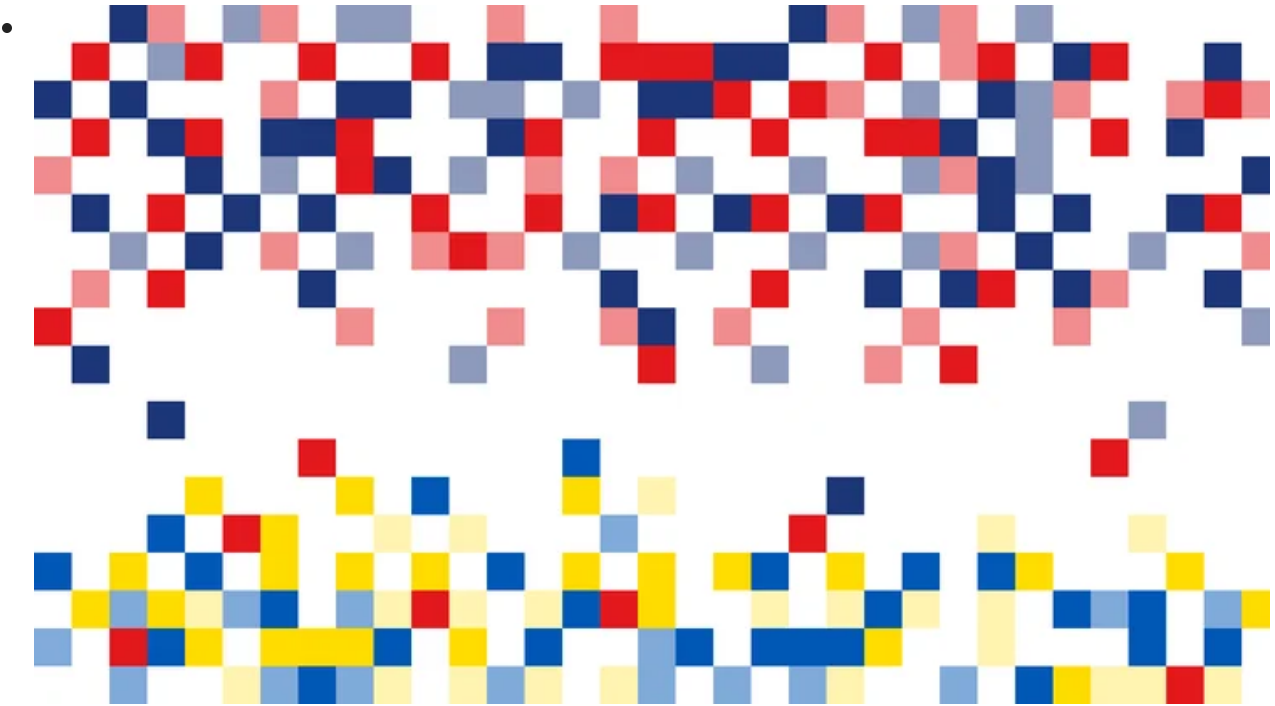
[Apr 05, 2023](#)

- [Threat Analysis Group](#)
[Magniber ransomware actors used a variant of Microsoft SmartScreen bypass](#)

[New research from Threat Analysis Group on Magniber's exploitation of Microsoft 0-day vulnerability.](#)

By [Benoit Sevens](#)

[Mar 14, 2023](#)



[Threat Analysis Group](#)

[Fog of war: how the Ukraine conflict transformed the cyber threat landscape](#)

[By Shane Huntley](#)

[Feb 16, 2023](#)

• [Threat Analysis Group](#)

[Over 50,000 instances of DRAGONBRIDGE activity disrupted in 2022](#)

[An update on TAG's work to disrupt the information operation network
DRAGONBRIDGE.](#)

[By Zak Butler Jonas Taege](#)

[Jan 26, 2023](#)

• .