# Case study: Watering hole attacks

June 2020

THE ENGINE ROOM

Internews

# Contents

# Introduction

The purpose of this case study is to illustrate the consequences of digital attacks against human rights and alternative media organisations, while recommending how such organisations–and practitioners from all backgrounds supporting them–may mitigate digital attacks.

This case study is one of three, which were prioritised based on a review of recent digital attacks and identification of which were most common. In creating these case studies, we reviewed documentation of community events, community research, interviews with digital security practitioners and responders conducted by The Engine Room, and incident trackers from the MONITOR regional support leads from April 2019 - March 2020. Further desk-based research was conducted on the specific type of attack to supplement each case study.

# What is a watering hole attack?

A watering hole attack involves an attacker, who is seeking to compromise the security of a specific group, infecting websites that members of that group are known to visit. The research group Citizen Lab defines watering hole attacks as, "a popular way to describe targeted malware attacks in which the attackers compromise a legitimate website and insert a "drive-by" exploit in order to compromise the website's visitors".[1]

The term is inspired by predators in the wild who prowl around watering holes, where their prey gather to hydrate. The digital version does just that–an attacker infects a website that members of a targeted group are known to visit, and when those members visit the compromised site, it infects their devices and/or computer networks with malware.[2] In this case, the malware is most likely surveillanceware, which is designed to capture and transmit sensitive user information like SMS messages, voicemails and phone conversations. Unlike spyware, surveillanceware targets specific individuals or organisations.[3] A watering hole attack is designed with a clear target group in mind, unlike spyware that aims to collect data on a vast number of unlucky random targets.

It is important to note that surveillanceware can also infect devices and computer networks through other means, like spear-phishing or via an attacker's physical access to a device. Watering holes attacks are just one of the ways surveillanceware is delivered to its targets.

What makes these attacks particularly insidious is that they infect websites that are trusted by a community or a group of people, but not controlled by them. This makes this digital security attack much harder to detect or avoid, in part because groups and organisations cannot monitor websites that do not belong to them for malicious behavior.

---

[1] https://citizenlab.ca/2012/10/watering-holes-and-zero-day-attacks/

[2] Malware can mean any kind of malicious software.

[3] *Lookout* "Mobile Security Glossary" https://www.lookout.com/know-your-mobile/glossary (Date accessed: 29 April 2020)

# Third-Party App Stores and watering hole attacks

In May 2018, Lookout Security Intelligence reported[4] on the discovery of a set of custom Android and iOS surveillanceware tools, which they respectively called Stealth Mango and Tangelo. Together with phishing and gaining physical access to the devices, using watering hole attacks was a key tactic used to deploy this malware.

As Lookout analysed exfiltrated data, they were able to pinpoint at least one of the watering holes at secure-apps.azurewe bsites[.]net–a URL pretending to be the third-party Android app store APKMonk. Links on the site either fail or re-direct the visitor to the Stealth Mango APK, which was disguised with fake information to get the user to download the app.[5]

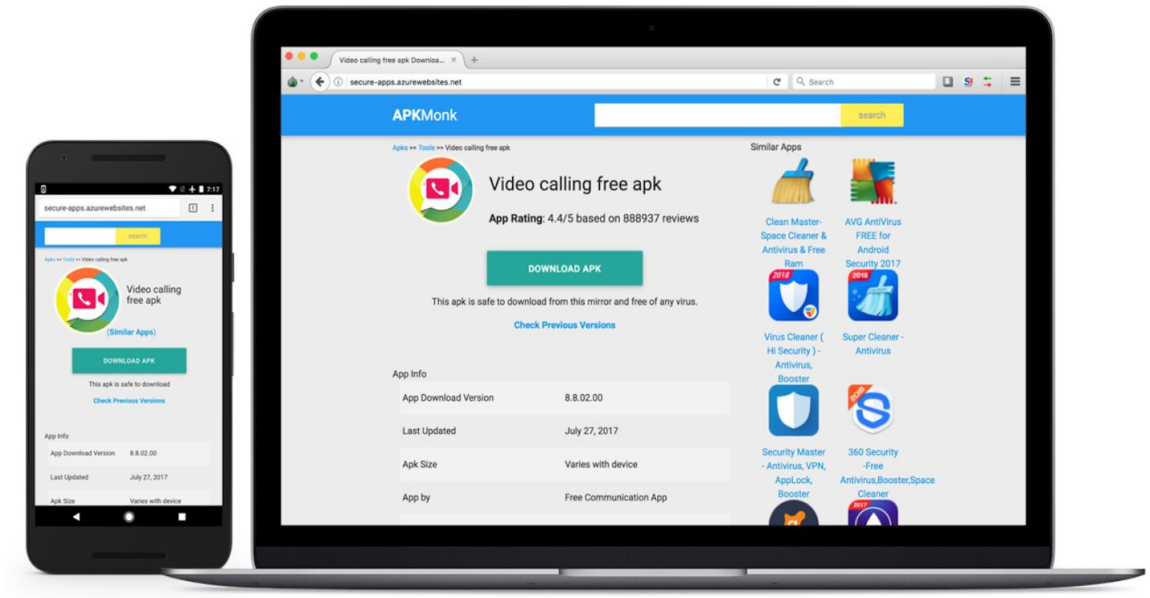


*Image: The watering hole as seen from desktop and mobile browsers ("Security Research Report: Stealth Mango and Tangelo" Lookout).*

[4] https://blog.lookout.com/stealth-mango

[5] "Security Research Report: Stealth Mango and Tangelo" *Lookout* https://info.lookout.com/rs/051-ESQ-475/images/lookout-stealth-mango-srr-us.pdf 15 May 2018 (Date accessed: 15 April 2020)

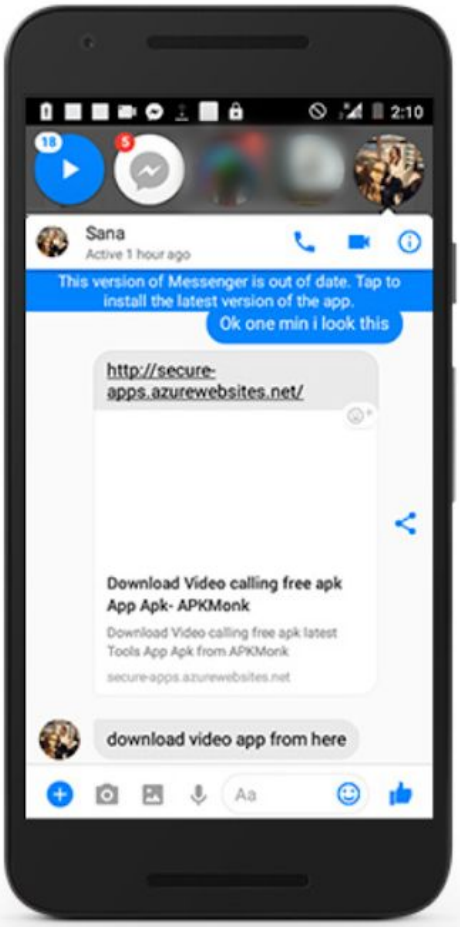


*Image: A screenshot of an infected Android device that shows the watering hole and the phishing attempt via Facebook Messenger. ("Security Research Report: Stealth Mango and Tangelo" Lookout).*

Lookout's Security Report indicates that all Stealth Mango samples launch their services at the highest priority possible, meaning the actions and processes it runs take prominence over other OS system and application tasks, and contain at least two background services which initially upload all data from an infected device and then track all changes that occur as soon as they happen. The malware also has categories for each type of information that, in later variants, is used as a model to create databases.[6] Later versions of Stealth Mango contain heightened functionality to further track victims in real time including obtaining root access to the device in order to ensure persistence as well as access the message databases of third-party social media applications.

According to Lookout, Stealth Mango and Tangelo are part of a targeted intelligence gathering campaign operated by members of the Pakistani military directed at government officials, members of the military, medical professionals and civilians in Pakistan, Afghanistan, India, Iraq, Iran, and the United Arab Emirates.The core targets were a mix of Pakistani government and military officials who had access to sensitive material and who were chosen for the purpose of espionage of said material

[6] Ibid.

# Detecting watering hole attacks

There are three main components to a watering hole attack.

The first consists of attackers conducting social engineering on the targets to know which websites they frequent and which of these sites are vulnerable. These websites could either be independently-run sites when the mainstream site is unavailable or fake sites created specifically to infect devices with malware. Other cases of watering hole attacks against activists and journalists have exploited smaller websites known to be visited by specific groups. Secondly, attackers identify and exploit a website's vulnerabilities (plug-ins that are not updated, for example).

After websites are exploited, they become sites to infect visitors' devices and networks with malware. This usually happens through zero-day vulnerabilities of computer software. A zero-day vulnerability is an unknown or unaddressed weakness in software programmes. Attackers exploit these vulnerabilities to infect a device or a network to which the device is connected.

Detecting a watering hole attack requires research from digital security analysts and experts and data from infected devices. Detection is particularly difficult because the waterhole attack can come from semi-trusted distribution channels, from community-trusted websites that have been hacked and from well-designed spoofed websites that trick users into downloading the surveillance-ware.

Attackers often demonstrate deep knowledge of the targeted groups, as shown in a surveillance campaign[7], carried out using chains of zero day iOS exploits to spy on iPhones likely owned by members of the Uyghur community. In this case, the websites that were compromised demonstrated extreme targeting of the Uyghur community and its supporters, with some being written in the Uyghur language, a somewhat rare language. In this case, the attack was allegedly discovered not by the target(s), but by Google's Threat Analysis Group (TAG)[8] and reported by Project Zero, a team of Google security researchers who study zero day vulnerabilities[9].

Understanding the root of the cause of an attack requires a collective effort and information sharing between trusted networks.

Sometimes it is easier to detect the malware that has infected a device or a computer network via the watering hole than it is to determine where the watering hole is. Being able to detect the malware that has infected a computer device or network, and then doing forensic work to back-trace the source of the malware, can potentially lead to the watering hole. However, it's important to note that detection of advanced surveillanceware is not as easy as detecting other kinds of common malware. Advice on malware detection and analysis can be found on Access Now's Digital First Aid Kit, under the title "My Device is Acting Suspiciously."[10] Practitioners looking to triage potential advanced threats can follow the Access Now Helpline's public documentation.[11] More advice for practitioners on collecting indicators of

[7] https://www.eff.org/deeplinks/2019/09/watering-holes-and-million-dollar-dissidents-changing-economics-digital
[8] https://googleprojectzero.blogspot.com/2019/08/a-very-deep-dive-into-ios-exploit.html
[9] https://googleprojectzero.blogspot.com/p/about-project-zero.html
[10] https://digitalfirstaid.org/en/topics/device-acting-suspiciously/
[11] https://communitydocs.accessnow.org/258-Advanced_Threats_Triage_Workflow.html

compromise and beginning analysis can be found on SAFETAG[12] and in the Threat Analysis and Sharing Webinar series Internews hosts.[13]

Besides investigating the infected target device, web maintainers and hosters who are managing the infected websites can also help to detect a watering hole attack. Ideally, they have the ability to know if their site's security has been compromised or have access to experts who can assist them.

# Impact of watering hole attacks

Watering hole attacks result in a person or a group's data becoming compromised, and in some cases, a significant breach in their privacy and security.

Through Stealth Mango and Tangelo, the perpetrators gained access to over 15 gigabytes of data from government officials, members of the military, medical professionals and civilians' infected devices, including letters and internal government communications, detailed travel information, pictures and IDs, GPS coordinates of pictures, pictures of closed-door meetings, and other information relevant to espionage activities.[14] In five months of analysis by Lookout (January to May 2018), the attackers had retrieved at least 30 thousand images, 6 thousand call recordings, 600 videos and dozens of environment recordings.[15]

According to Lookout's report, Stealth Mango was deployed against victims in Pakistan, Afghanistan, India, Iraq, Iran and the United Arab Emirates. The surveillanceware also retrieved sensitive data from individuals and groups in the United States, Australia and the United Kingdom.

On a personal level, it has an impact on an individual and a group's sense of security and safety. As with spear-phishing, which is another type of targeted attack that gains access to sensitive information, there is also a threat to community trust in the face of a watering hole attack. The sense of not knowing whose devices have been breached and whose security has been compromised has a negative effect on a group, network, community or movement.

If the community members feel they can't trust platforms and news sites that they need to do their work, they will stop participating in those spaces. They may also be suspicious of new connections made on these platforms, even if the connection is initiated by a legitimate ally. Paranoia and loss of trust are commonly cited reasons for the dissolution of social movements, to the extent that law enforcement and governments integrate this into their strategies and tactics. If an activist is struggling, they may be less likely to ask for help if they can't trust the contacts and digital spaces they have access to.

In the case of the zero-days used to target visitors to Uyghur-language websites, the attack[16], "represents a sea-change in how zero-days are being used; while China continues to target specific

---

12 https://safetag.org/guide/#section2.13

13 https://globaltech.internews.org/blog/help-website-hacked

14 Blake, Andrew and Flossman, Michael. *Lookout* "Stealth Mango and Tangelo: Nation state mobile surveillanceware stealing data from military & government officials" https://blog.lookout.com/stealth-mango 15 May 2018 (Date accessed: 15 April 2020)

15 https://www.slideshare.net/cisoplatform7/stealth-mango-and-the-prevalence-of-mobile-surveillanceware

16 https://www.volexity.com/blog/2019/09/02/digital-crackdown-large-scale-surveillance-and-exploitation-of-uyghurs/

high-profile individuals in spear-phishing campaigns, they are now unafraid to cast a much wider net, in order to place their surveillance software on entire ethnic and political groups outside China's border".[17]

Because of the nature of the information captured by surveillanceware, those who have been compromised also may experience threats to their physical security. Some of the sensitive information that surveillanceware can access could contain geographical locations of individuals, their daily schedules and travel details–information that can be used for physical surveillance and/or to physically attack an individual.

# Mitigation strategies and tactics

There are ways to mitigate the consequences of a watering hole attack.

At an individual level:

- Keep your software and apps updated. Watering hole attacks exploit holes and vulnerabilities from out-of-date software to infiltrate devices. Consider making it a habit to check for app updates or for available security patches from developer websites.
- Practice safe application installation principles. Don't install apps that ask for more permissions than necessary to operate (for example, a notepad app should not need access to your address book or your network settings). Don't install apps that require full access to your device in order to work.
- Don't download and install applications from unknown and illegitimate sources, whenever possible. Do your own research if you haven't received the application from a trusted and knowledgeable source. When in doubt, don't download the app until you ask for advice from groups like Access Now Helpline.
- Hide your online activities, especially anything related to your activism, by clearing your browser trackers and using a VPN or the Tor Browser to access the internet. Watering hole attacks are effective because attackers target websites that they know you and your group visit.
    - For more information about choosing a VPN check out Electronic Frontier Foundation's (EFF) guide.[18]
    - To learn about web browsing security, read EFF's documentation.[19]
    - AccessNow also has documentation about safer browsing practices[20] and circumvention of censorship.[21]
- Other ways to consider hiding your activities online can be not publicising which sites your visit on your social media spaces, making your social media private and using secure communication channels to discuss your online activities with those that you trust.
- Along with your anti-virus, have anti-malware software like Lookout on your mobile phones, or Malwarebytes for different devices. Anti-virus protects against older, more established threats, such as Trojans, viruses, and worms. Anti-malware focuses on newer threats, such as malware delivered by zero-day exploits. Many groups, like MalwareBytes, recommend installing both for better coverage.[22]

---

[17] https://www.eff.org/deeplinks/2019/10/chinas-global-reach-surveillance-and-censorship-beyond-great-firewall
[18] https://sec.eff.org/topics/VPN
[19] https://sec.eff.org/articles/web-browsing-security
[20] https://communitydocs.accessnow.org/212-Safe_Browsing_Practices.html
[21] https://communitydocs.accessnow.org/175-Circumvention_Anonymity_tools_list.html
[22] https://blog.malwarebytes.com/101/2015/09/whats-the-difference-between-antivirus-and-anti-malware/

At an organizational or group level:

At an organizational or group level–including within groups, networks, communities and movements–consider standardizing these practices across the organisation, and develop policies and protocol accordingly:

- Consider hiring an IT support manager to help you and your team have updated systems and monitor your networks. Ideally, this person would support in advising on or running network security tools. For example, considering intrusion prevention systems and bandwidth management software will enable you to observe user behavior and detect abnormalities that could indicate an attack, such as large transfers of information or a high number of downloads.
- If you are maintaining the organisation's website, regularly monitor your network activity. Watch out for unusual traffic in your network–such as large file uploads–as it could indicate malware present in the system. If you don't maintain your own website, ask your web host if they have easy-to-use ways of monitoring traffic on your site
- Monitor your devices for presence of surveillanceware. These characteristics may indicate presence but are not definitive:
    - Devices being slow or sluggish.
    - The battery runs out faster than usual, even if you are idle or not doing anything more than usual.
    - Applications launching without prompting from you.
    - Your internet traffic is heavier than usual.
    - You receive more phishing messages than usual.

# Other considerations

As surveillance-ware gets more sophisticated, it becomes harder to detect without digital security forensics skills. As these threats evolve, it is important that potentially targeted organizations/communities and digital security practitioners stay vigilant and informed about new threats.

The mechanics of watering hole attacks also raises questions about the responsibility of intermediaries whose sites are hijacked to carry out the attack. While they are not complicit with the attackers, their weaknesses become threats to others. Though they may not directly work with members of a vulnerable community, they would ideally harden their web services, or have access to experts who can assist them, in order to protect communities from "drive by" watering hole attacks.

# Resources

- https://blog.lookout.com/stealth-mango
- https://www.amnesty.org/en/latest/news/2018/05/pakistan-campaign-of-hacking-spyware-and-surveillance-targets-human-rights-defenders/
- Human Rights Under Surveillance: Digital Threats against Human Rights Defenders in Pakistan https://www.amnesty.org/en/documents/asa33/8366/2018/en/
- A Primer on Watering Hole Attacks: https://www.paralleledge.com/a-primer-on-watering-hole-attacks/
- Beware of Stalkware: https://securelist.com/beware-of-stalkerware/90264/

- How to Tell if Your Computer is Being Monitored: https://helpdeskgeek.com/how-to/5-ways-to-make-sure-no-one-is-monitoring-your-computer/
- Is Someone Spying on Your Cellphone? 10 Ways to Tell and Stop them https://pixelprivacy.com/resources/spying-on-your-cell-phone/
- Watering Holes and Million Dollar Dissidents: the Changing Economics of Digital Surveillance https://www.eff.org/deeplinks/2019/09/watering-holes-and-million-dollar-dissidents-changing-economics-digital
- https://googleprojectzero.blogspot.com/2019/08/a-very-deep-dive-into-ios-exploit.html
- https://duo.com/decipher/russian-attackers-used-iranian-infrastructure-and-tools-against-multiple-targets
- https://citizenlab.ca/2012/10/watering-holes-and-zero-day-attacks/
- https://citizenlab.ca/2016/01/citizen-lab-palo-alto-networks-scarlet-mimic/
- Communities @ Risk, Targeted Digital Threats Against Civil Society https://targetedthreats.net/