EKOPARTY #PWNDEMIC 2020

THREAT SUMMARY REPORT

STALKERWARE 09/26/20

SUMMARY

On September 26th, 2020, a presentation, “Every Breath You Take: A CTI Review of Stalkerware,” at Ekoparty provided insights into Stalkerware concerning what it is, how it works, who it targets, how stalkerware could impact Enterprise companies, and possible solutions to consider.

Stalkerware is software used to “facilitate intimate partner intimate partner violence, abuse, or harassment, including pernicious intrusions into the targeted person’s life by way of physical or digital actions” [1]. Commodity stalkerware is a tool used for intimate partner surveillance along with commodity spyware, dual-use apps, shared accounts, IOT devices, home security services, mRATs, and more. Stalkerware could be considered spyware, stalkerware, dual-use apps, or mRATs based upon their respective usage.

TECHNICAL SUMMARY

Capabilities of Commodity Stalkerware

- Basic: review text messages, various chat applications (WhatsApp, LINE), phone call logs, GPS location, browser history, stored media such as photos and videos [1].
- Varies by Stalkerware Vendor: access to email, social media, additional messaging apps, device settings, stored files, record phone calls, voicemails, calendar, contacts, record surroundings, keystrokes, take pictures [1].

Lockheed Martin Cyber Kill Chain of Commodity Stalkerware

- Reconnaissance
  - Information gathering on target
- Weaponization
  - Obtain url or other instructions for stalkerware installation through purchasing the service.
- Delivery
  - Obtain physical access to the targeted device.
- Exploitation
  - No technical exploits for commodity Stalkerware
  - Possible social engineering of target
  - Unlock screen, if locked.
  - Determine access to download apps from the App Store/Google Play Store, or modify settings of the phone.
    - Leverage remote support of stalkerware vendor to install stalkerware
- Installation
  - Install stalkerware via stalkerware vendor provided link, stalkerware vendor provided instructions, or via app store.
- Command and Control
  - Remote Access to device over Wifi or Cell and contents displayed on a web-based GUI for the operator

- Actions on Objectives
    - Unauthorized access to data on phone, exfil data, modify data

MITRE ATT&CK
- Mobile tactics and techniques available related to stalkerware found [10]
    - T1461, T1475, T1412, T1468, etc.

CTI ANALYSIS

The threat to the organization is currently a **LOW***.

Based upon the operating system of corporate cell phones and phones that are managed mobile devices, it would be necessary to review the installation process and any available technical manuals of stalkerware specific to the phones.

*The threat level may increase if a company has a "BYOD" policy or does not leverage a mobile device management solution.

Potential Threat of Repurposed Stalkerware Tactics Applied to Corporate
- Insider Threats
- Executives/Employees [2]
- Competitors
- Industrial Espionage [2]

Potential Threat of Stalkerware to Corporate
- Stalkerware possibly able to circumvent or leverage compromised mobile device management solutions [18] [19] [20]
- Stalkerware and BYOD considerations
- Stalkerware Vendors: Security practices, misconfigs, breaches, etc [1] [2] [11] [12] [13] [14] [15] [16] [17]

Potential RFIs to Other Teams
- Determine how Mobile Device Management solutions are impacted by stalkerware/mRAT.
- Determine how BYOD is impacted by stalkerware/mRAT.
- Determine if it is possible to convert a smartphone to a mobile pentesting device and a remote attacker via Stalkerware could potentially pivot to IOT devices or printers on the corporate network, etc.
    - Determine if it's possible to pivot to corporate network via stalkerware remote access without the phone being turned into a pentesting device.

Potential Solutions
- CTI: Block exfil domains at proxy, suggest to disallow rooted phones on corporate network, discover if detection is possible for nation-state influenced apps and create a custom alert based upon data exfil threshold, suggest to disallow use of nation-state influenced apps such as WeChat and TikTok, etc [1] [2] [8] [9]
- Awareness campaigns and training for employees
    - Cell phone security tips [3] [11]
        - Don't leave smartphone unattended, delete unused apps, regularly search for suspicious apps and activity on phones, use quality password manager, don't

share passwords, lock cell phone screen, change passcode frequently, review privacy settings and access to social media accounts including active sessions, set up 2FA on every account possible, etc [3]
        - Android: check device administrators, if Google Play Protect is disabled or if install apps from unknown sources is enabled this could be a sign of stalkerware. [11]
        - Apple: Jailbroken or review account information of iCloud account [11]
    - Existing AV and anti-spyware tools are ineffective at detecting and remediating stalkerware and dual-use apps are not flagged [1] [4]
    - Travel safety tips for executives/employees with access to sensitive data [2]
    - Stalkerware Lunch-n-Learns or Company Sponsored Meetings
- Resources for employees that are concerned about stalkerware
    - Cornell Tech
        - Client-centered Clinical Computer Security Practice [5]
            - Cornell Privacy Checkup Worksheet [6]
            - Cornell Spyware Scanning Tool [7]
    - Tallpoppy.io
    - NCADV.org
    - NNEDV.org
    - SafeEscape.org
    - StopStalkerware.org
- TableTops on how to monetize your specific org's data exfil by stalkerware capabilities. Is a breach of a stalkerware vendor with your Org's data considered a breach of your org? In the event of poor security practices or misconfigs of the stalkerware vendor and your org's sensitive data is publicly exposed, how would your org address a take-down request when there isn't a policy in place at the stalkerware vendor to address the targets' take-down requests? What will you do if ransomware operators attempt to extort your org from data/information obtained from stalkerware? Where is your MDM server/Solution and is there detection/alerts/defense-in-depth for it? What would be the worst case scenario if your MDM server was compromised and spyware was sent out to 75%+ of mobile devices? [1] [19] [20]

Targets
- Relationships
- Targets of similar functionality to stalkerware
    - children, employees, journalists, dissidents, activists, citizens, religious leaders, criminals, terrorists, military, governments, government officials, law enforcement

Operators
- Relationships
- Operators using similar functionality to stalkerware
    - parents, schools, companies, cybercrime, hacktivists, criminals, terrorists, law enforcement, governments, nation-states

TIMELINE
9/26/20: Ekoparty

IOCS

- Recent Crowd Sourced IOCs: https://github.com/ch33r10/Stalkerware
- Provided by The Citizen Lab, The Predator In Your Pocket p 37-38
    - Last checked September 2018 by The Citizen Lab [1]

REFERENCES

[1] https://citizenlab.ca/docs/stalkerware-holistic.pdf
[2] https://securityintelligence.com/articles/when-stalkerware-stalks-the-enterprise/
[3] https://stopstalkerware.org/2019/10/06/the-stalkerware-threat/
[4] https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8418618
[5] https://havron.dev/pubs/clinicalsec.pdf
[6] https://www.ipvtechresearch.org/resources
[7] https://github.com/stopipv/isdi
[8] https://www.cyberscoop.com/u-s-army-bans-tiktok-amid-ongoing-scrutiny-chinese-made-video-app/
[9] https://www.wsj.com/articles/chinas-tech-giants-have-a-second-job-helping-the-government-see-everything-1512056284
[10] https://attack.mitre.org/techniques/mobile/
[11] https://github.com/diskurse/android-stalkerware
[12] https://twitter.com/lorenzofb/status/1057679550790934528
[13] https://www.vice.com/en_us/article/7xnybe/hosting-provider-takes-down-spyware-mobiispy
[14] https://www.vice.com/en_us/article/9kmj4v/spyware-company-spyfone-terabytes-data-exposed-online-leak
[15] https://www.vice.com/en_us/article/53vm7n/inside-stalkerware-surveillance-market-flexispy-retina-x
[16] https://www.vice.com/en_us/article/gvye3m/spy-tech-company-hacking-team-gets-hacked
[17] https://www.vice.com/en_us/article/z4mzze/a-hacker-claims-to-have-leaked-40gb-of-docs-on-government-spy-tool-finfisher
[18] https://www.usatoday.com/story/tech/2019/10/08/is-the-boss-tracking-you-now/3901594002/
[19] https://threatpost.com/cerberus-trojan-major-spyware-targeted-attack/155415/
[20] https://blog.orange.tw/2020/09/how-i-hacked-facebook-again-mobileiron-mdm-rce.html?m=1

RESEARCH

https://citizenlab.ca/2018/09/hide-and-seek-tracking-nso-groups-pegasus-spyware-to-operations-in-45-countries/
https://www.ipvtechresearch.org/research
https://www.zdnet.com/article/employee-safety-is-for-sale/
https://www.vice.com/en_us/article/ywqqkw/military-fbi-and-ice-are-customers-of-controversial-stalkerware
https://citizenlab.ca/docs/stalkerware-holistic.pdf
https://www.wired.com/story/eva-galperin-stalkerware-kaspersky-antivirus/
Heather Mahalik https://youtu.be/IEbLOvT4Fts
Eva Galperin https://youtu.be/QvorPIKXrYA
Eva Galperin TED Talk https://youtu.be/xzWFrHHTrs8
https://assets.documentcloud.org/documents/4599753/NSO-Pegasus.pdf
https://www.nytimes.com/2019/12/22/us/politics/totok-app-uae.html
https://www.nytimes.com/2019/11/06/opinion/whatsapp-nso-group-spy.html
https://www.digitalbank.global/nso-group-competitors
https://www.fastcompany.com/90369108/inside-the-shadowy-world-of-spyware-makers-that-target-activists-and-dissidents
https://sii.transparencytoolkit.org/search?technology_sold_facet=Phone+Monitoring
https://www.calcalistech.com/ctech/articles/0,7340,L-3749924,00.html
https://www.washingtonpost.com/opinions/2018/12/05/israel-is-selling-spy-software-dictators-betraying-its-own-ideals/
https://www.vice.com/en_us/article/qvakb3/inside-nso-group-spyware-demo
https://www.vice.com/en_us/article/3da5qj/government-hackers-iphone-hacking-jailbreak-nso-group
https://www.welivesecurity.com/2018/06/07/invisimole-equipped-spyware-undercover/
https://arsenalexperts.com/persistent/resources/pdf/Illicit_Surveillance_of_Electronic_Systems_in_Family_Law_Cases.pdf
https://www.technologyreview.com/2019/07/10/134249/stalkerware-apps-are-letting-abusive-partners-spy-on-their-victims/
https://www.zdnet.com/article/the-ultimate-guide-to-finding-and-killing-spyware-and-stalkerware/
How to Fake a Fingerprint https://youtu.be/tj2Ty7WkGqk
https://www.zdnet.com/article/google-cleans-out-stalker-apps-from-play-store/

https://ivrodriguez.com/analyzing-ios-stalkerware-apps/
https://blog.talosintelligence.com/2019/10/the-commoditization-of-mobile-espionage.html
https://www.technologyreview.com/profile/patrick-howell-oneill/
https://www.vice.com/en_us/contributor/lorenzo-franceschi-bicchierai
https://blog.malwarebytes.com/malwarebytes-news/2019/11/malwarebytes-teams-up-with-security-vendors-and-advocacy-groups-to-launch-coalition-against-stalkerware/
https://www.ft.com/content/263133ac-a28b-11e9-974c-ad1c6ab5efd1
https://www.rsaconference.com/industry-topics/podcast/threats-of-surveillance-tools-spyware-and-stalkerware?
https://homeland.house.gov/preparing-for-the-future-an-assessment-of-emerging-cyber-threats
https://pages.cs.wisc.edu/~chatterjee/ppts/IPV_spyware.pdf
https://havron.dev/pubs/clinicalsec.pdf
https://havron.dev/pubs/freed-cscw19.pdf
http://nixdell.com/papers/stalkers-paradise-intimate.pdf
http://nixdell.com/papers/a046-freed.pdf
https://www.technologyreview.com/s/614168/nyc-hires-hackers-to-hit-back-at-stalkerware/
https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8418618
http://damonmccoy.com/papers/Creepware_SP.pdf
https://www.vice.com/en_us/topic/when-spies-come-home
https://citizenlab.ca/docs/stalkerware-legal.pdf
https://www.theguardian.com/world/2019/dec/20/cyprus-police-arrest-three-in-israeli-owned-spy-van-investigation
https://info.lookout.com/rs/051-ESQ-475/images/lookout-pegasus-technical-analysis.pdf
Cian Heasley BSides London 2019 Watching the Watchers: The Stalkerware Surveillance Ecosystem https://youtu.be/EzMkqtNAo6A
https://www.defcon.org/images/defcon-20/dc-20-presentations/Robinson/DEFCON-20-Robinson-Spy-vs-Spy.pdf
http://www.structuredweb.com/sw/swchannel/CustomerCenter/documents/9353/25297/Lacoon_CP_Enterprise_mRAT_Research.pdf
Jessica Amery BSides London 2019 Stalkerware in Mobile Devices https://youtu.be/liUFxUChJcI
https://www.rsaconference.com/industry-topics/blog/tracking-every-move-from-location-based-apps-to-stalkerware-and-advanced-attacker
https://www.nytimes.com/interactive/2019/12/19/opinion/location-tracking-cell-phone.html
https://googleprojectzero.blogspot.com/2019/08/a-very-deep-dive-into-ios-exploit.html
https://www.researchgate.net/publication/340588456_Decompiled_APK_based_malicious_code_classification
https://www.blackhat.com/html/webcast/05072020-stalkerware-solutions-for-mitigating-its-impact-on-privacy-and-security.html
https://threatpost.com/cerberus-trojan-major-spyware-targeted-attack/155415/
https://www.cbc.ca/news/opinion/opinion-stalkerware-abuse-covid-isolation-phones-1.5556379
https://www.vice.com/en_us/article/8899nz/nso-group-pitched-phone-hacking-tech-american-police
https://www.vice.com/en_us/article/n7wna7/lapd-phone-hacking-nso-group-westbridge
https://thehackernews.com/2020/04/iphone-zero-day-exploit.html
https://www.bloomberg.com/news/features/2020-03-27/bosses-panic-buy-spy-software-to-keep-tabs-on-remote-workers
https://thehackernews.com/2020/03/iphone-iOS-spyware.html
https://www.businessinsider.com/us-government-agencies-have-banned-tiktok-app-2020-2
https://www.zdnet.com/article/stalkerware-infections-grew-by-40-in-2019-says-kaspersky/
https://www.cnet.com/news/how-schools-may-use-kids-phones-to-track-and-surveil-them/
https://techcrunch.com/2020/02/20/kidsguard-remove-stalkerware/
https://techcrunch.com/2020/02/20/kidsguard-spyware-app-phones/
https://blog.malwarebytes.com/stalkerware/2020/03/international-womens-day-awareness-of-stalkerware-monitoring-and-spyware-apps-on-the-rise/
https://medium.com/@nickkshepard/the-continued-rise-of-stalkerware-eba471d851a4
https://www.cnet.com/news/1-in-10-people-uses-stalkerware-to-track-partners-and-exes-poll-says/
https://www.cnet.com/news/stalkerware-what-to-know-when-youre-the-target/
https://threatpost.com/stalkerware-extra-creepy-features/153874/
https://securityaffairs.co/wordpress/96295/malware/joker-malware-actiity.html
https://securityaffairs.co/wordpress/98279/malware/joker-malware-play-store.html
https://www.techradar.com/news/stalkerware-poses-higher-privacy-risk-than-ever-heres-what-you-need-to-know
https://www.refinery29.com/en-us/spyware-stalkerware-dangers
https://wfhb.org/news/better-beware-stalkerware/
https://blog.avast.com/the-stalkerware-threat-avast
https://eandt.theiet.org/content/articles/2020/03/lurking-in-the-shadows-the-disturbing-rise-of-stalkerware/
https://vpnoverview.com/news/monitorminor-new-super-stalkerware/
https://www.infosecurity-magazine.com/news/stalkerware-soared-91-in-uk-last/

https://www.securityweek.com/rare-android-stalkerware-can-steal-data-control-devices
https://the-parallax.com/2020/02/18/stopping-stalkerware-confounds-experts/
https://www.techdirt.com/articles/20200220/14571543957/stalkerware-developer-found-leaking-sensitive-data-thousands-softwares-victims.shtml
https://www.pcmag.com/news/ftc-blocks-us-company-from-selling-stalkerware-apps
https://www.usenix.org/conference/enigma2020/presentation/galperin
https://citizenlab.ca/2020/01/stopping-the-press-new-york-times-journalist-targeted-by-saudi-linked-pegasus-spyware-operator/
https://www.nytimes.com/2020/01/22/technology/jeff-bezos-hack-iphone.html
https://www.reuters.com/article/us-davos-meeting-saudi-arabia/saudi-foreign-minister-calls-claim-that-crown-prince-hacked-bezos-phone-absurd-idUSKBN1ZL1ED