No images? Click here

Monitoring the Cloud

Brian J. Kelly, Cyber Analyst - IPPC Technologies

The 21st century has brought the world many things, but none more impactful than the expansion of technology. The world of personal computing has evolved to the “Internet of Things” (IoT) bringing multiple connected devices into the home and allowing users to access, share and store the gamut of content. According to a recent survey by Deloitte, U.S. households have 22 connected devices, on average. The challenge for officers when managing a person under supervision for a computer/Internet-related crime is not only addressing multiple Internet-capable devices in the home but also that evidence is no longer confined to a physical device. For example, an examination of a mobile device, such as a Samsung Galaxy (Android

OS) mobile phone, following suspected violation conduct, may only uncover indicators of various activity (i.e. social media profile IDs; email addresses) but not the full content of an Internet account, such as photos, videos, private messages, etc. Officers must also be well-versed of procedural, evidentiary and legal concerns if examining a device still connected to the Internet. Examining a device while connected to the Internet could result in examination of evidence outside the scope of search authorization along with changes in digital evidence. In response, a few years ago as an officer, I formulated the following special condition language to track, monitor and allow for the examination of Internet accounts:

The defendant shall report to the Probation Office any and all electronic communications service accounts (as defined in 18 USC 2510(15)) used for user communications, dissemination and/or storage of digital media files (i.e. audio, video, images). This includes, but is not limited to, email accounts, social media accounts, and cloud storage accounts. The defendant shall provide each account identifier and password, and shall report the creation of new accounts, changes in identifiers and/or passwords, transfer, suspension and/or deletion of any account within 5 days of such action. Failure to provide accurate account information may be grounds for revocation of release. The defendant shall permit the Probation Office to access and search any account(s) using the defendant's credentials pursuant to this condition only when reasonable suspicion exists that the defendant has violated a condition of his supervision and that the account(s) to be searched contains evidence of this violation. Failure to submit to such a search may be grounds for revocation of release.

This condition could be used in combination with computer & Internet monitoring as part of an overall computer & Internet management/monitoring program or as a stand-alone condition when device monitoring is not needed or desired. As indicated in the condition, the targets are typically Internet service provider accounts where the crucial data is stored in the cloud on the provider's servers. Key Internet providers are social networks (i.e. Facebook, Instagram), email providers (i.e. Yahoo, Gmail) and cloud storage (i.e. Dropbox). While an officer could use open source intelligence (OSINT) tools to discover social network profiles or email addresses, there are limitations to what can be uncovered. Properly configured privacy settings, private messaging, etc. are some of the challenges when attempting to obtain and verify information. There are also concerns with an officer creating fictitious or undercover profiles, which could violate terms of service agreements of the providers and result in such accounts being purged. There are commercial tools available that offer to collect and search data from Internet service providers, but the strength of these tools are typically in the reporting and storage of downloaded content. An officer still would need to not only know the account/profile information, but also need the user credentials and authority to access and download the information. Another obstacle of community correction agencies can be the limited ability to obtain legal process such as subpoenas. In the federal system, law enforcement agencies under the Executive Branch have the ability to generate administrative subpoenas as an investigative tool. The U.S. Probation Office, which is part of the Judicial Branch and did not have this authority, did have the ability to request a court order under the All Writs Act from an U.S. District Court Judge, but this process was used very sparingly.

There are a number of tools and techniques for specific providers that officers can use to obtain information, but these are constantly changing in response to efforts by providers to combat the ability for non-users to search their databases. For the most current tools, simply conduct a search for "OSINT tools" or similar terms. See below for helpful links:

- OSINT Guides: https://www.skopenow.com/resource-center
- OSINT Framework: https://osintframework.com/
- Gramhir (Instagram analyzer and viewer; does not require account): https://gramhir.com/
- CentralOps (Network tools such as Whois): https://centralops.net/co/

Capturing web-mail and social media private messaging when monitoring a device can be a challenge due to proprietary code used by the providers. Routing email through email clients like Microsoft Outlook (not Outlook.com) utilizes standard protocols such as IMAP, SMTP and POP3, so capture is more consistent. But private messaging via social networks cannot be routed through a client, therefore a combination of device monitoring and an Internet account search condition would be a more complete approach. Utilizing a special condition as suggested above from the start of supervision allows officers to establish a baseline of information on the individual being supervised. Throughout supervision, in conjunction with information obtained from computer/Internet monitoring data and/or digital forensic examinations, officers can properly manage and monitor the usage of Internet accounts during the course of supervision.

IPPC's computer & Internet monitoring solutions, which include robust artificial intelligence tools, and services such as Spotlight and Express Scan, will assist officers throughout the supervision process. IPPC can assist in locating and isolating Internet account identifiers such as profile IDs, screen names, email addresses, user credentials, etc. which can be used to verify reported information. For example, officers running Windows Express Scan from a toolkit (USB) have the option to attempt credential capture. Windows Express Scan will look to identify any web browsers for which credentials have been saved and decrypt the credentials for plain-text view. If an officer does not elect to attempt credential capture Express Scan, by default, will still show any websites for which credentials are identified, but will simply skip the step of decryption of the credentials. For more information on Express Scan, please contact Phillip Danford at (919) 827-1230 or pdanford@ippctech.net. For more information on IPPC's services such as Spotlight, please call IPPC at (888)-WEB-IPPC or contact me directly at bkelly@ippctech.net or by calling (516)341-4201.

IPPC TECHNOLOGIES
PO BOX 60144
KING OF PRUSSIA, PA 19406
TEL: 888-WEB-IPPC (932-4772)
INFO@IPPCTECH.NET
WWW.IPPCTECH.NET