HELP NET SECURITY

Search Help Net Security

NEWS | MALWARE | ARTICLES | REVIEWS | Q&As | EVENTS | SOFTWARE | NEWSLETTER

Featured news

- More than 900 embedded devices share hard-coded certs, SSH host keys
- Four ways an attacker can infiltrate an organization by diverting security solutions
- GPS faker software broadcasts spam across thousands of fake profiles
- Linux crypto ransomware continues to wreak havoc, but there's some good news
- IBM cloud tool enables privacy-preserving user authentication
- MagSpoof: A device that spoofs credit cards, disables chip-and-PIN protection
- Another root CA cert with key found on Dell's machines
- ModPOS: The most sophisticated POS malware to date
- Amazon resets customers' potentially compromised passwords
- IoT attacks and evasion techniques will characterize threats in 2016
- Vonteera adware blocks AVs, can install uninstallable Chrome extensions
- How data protection regulations will affect the infosec industry
- Credential manager system used by Cisco, IBM, F5 has been breached
- Zero detection GlassRAT operated undetected for years
- Analytics services are tracking users via Chrome extensions
- Inside the largely unexplored world of mainframe security
- Ivan Ristic and SSL Labs: How one man changed the way we understand SSL

GPS faker software broadcasts spam across thousands of fake profiles

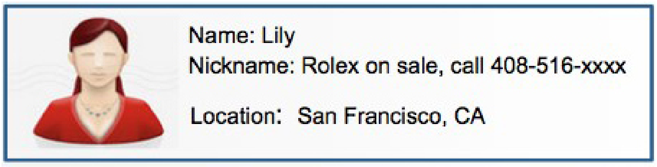
Posted on 26 November 2015.

Different from traditional email spam, social spam can reach a large audience by nature of the platform and can appear trustworthy since it is coming from people in your social network. This kind of spam also has a long lifespan since social media content stays online 24/7 and is rarely removed, if ever.

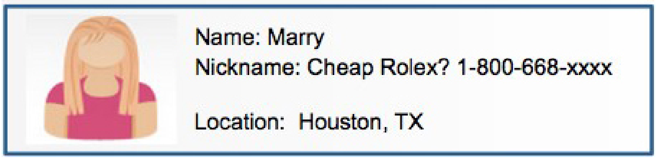
More than a mere annoyance factor, such attacks degrade brand name reputation and platform integrity, hindering user growth and even driving away existing users. This causes a stagnant user base and loss in ad revenue, which is what ultimately hits home for social media companies.

We recently observed malicious activities on a large social application that illustrate the ever-changing landscape of spam. Today, spam is commonly detected by content-based solutions which analyze messages. To evade this, the attackers chose not to post or send messages through traditional communication channels, thus these security solutions have no content to analyze.

Instead, spammy text was placed within the profile description of fake accounts. This hijacking of an app feature (that was not meant for messaging) for spam effectively allows attackers to evade vantage points used by existing security solutions.



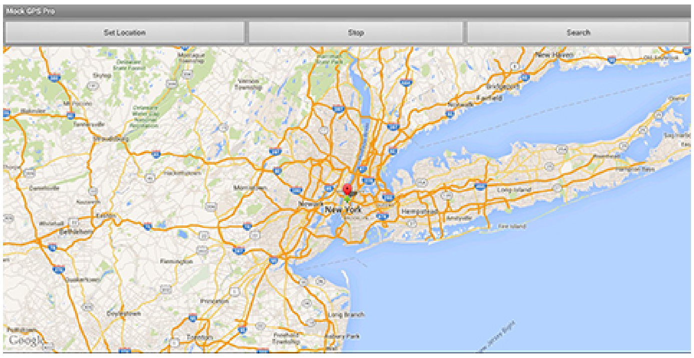
Name: Lily
Nickname: Rolex on sale, call 408-516-xxxx
Location: San Francisco, CA



Name: Marry
Nickname: Cheap Rolex? 1-800-668-xxxx
Location: Houston, TX

More ingenious is how the attackers exploited the location-proximity feature available on mobile apps to distribute spam. While such features enable users to find, view, and interact with others that are nearby, they also allow normal users that are close to the fake accounts to be spammed with the profile text. Using GPS faker tools, the spammers set the fake accounts' profile locations to span across tens of major cities to reach a large population of users.

The screenshot below shows an example of such a tool, Mock GPS. Users can drag anywhere in the map and select Set Location. Other apps on the device that subsequently attempt to read the device's GPS location will be given the specified value.



In addition to embedding malicious text in profile descriptions and manipulating GPS locations to distribute spam, this attack also exhibited

Spotlight

1 2 3 4 5

MagSpoof: A device that spoofs credit cards, disables chip-and-PIN protection

The device can wirelessly spoof credit cards/magstripes, disable chip-and-PIN protection, and predict the credit card number and expiration date of Amex cards after they have reported stolen or lost.

Weekly newsletter

Reading our newsletter every Monday will keep you up-to-date with security news.

Email @ Address | Subscribe

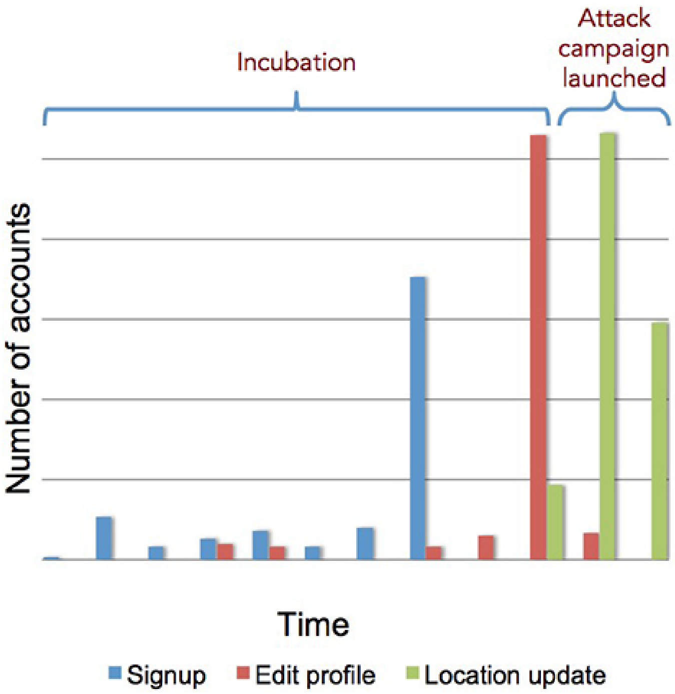
Daily digest

Receive a daily digest of the latest security news.

Email @ Address | Subscribe

an extended incubation period, making detection even more difficult.

Attackers spent several weeks preparing the accounts, including registering fake accounts and editing their profile information in small doses. These sleeper cell accounts can circumvent detection for months or years, appearing perfectly benign until right up to attack launch - in this case, spamming nearby users. At that point, the damage is already done.



The timeline of a spam attack with an extended incubation period. The attackers embedded spam messages in profile descriptions, and used GPS faker apps to set the fake accounts' locations to arbitrary cities.

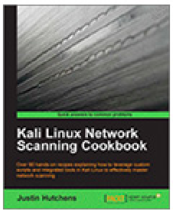
A problem with costly consequences

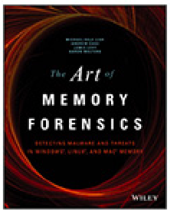
Social spam is not new, neither is profile spam. However, this example illustrates how cyber attackers are constantly devising new techniques to evade detection, just as online services are adopting new disruptive features to attract more users.

This is a costly problem that desperately needs advanced, predictive security solutions that can detect these hidden accounts masquerading as legitimate users. With evolving attack techniques that are becoming increasingly sophisticated, traditional reactive security solutions are forced to play an endless game of whack-a-mole to try to stop them. It's faking GPS this time, what's next?

Author: Ting-Fang Yen, Research Scientist at DataVisor.

cybercrime scams spam





DON'T MISS
Thu, Nov 26th

900+ embedded devices share hard-coded certs, SSH host keys

GPS faker software broadcasts spam across thousands of fake profiles

MagSpoof: A device that spoofs credit cards, disables chip-and-PIN

Inside the largely unexplored world of mainframe security

Ivan Ristic and SSL Labs: How one man changed the way we understand SSL

Back to TOP