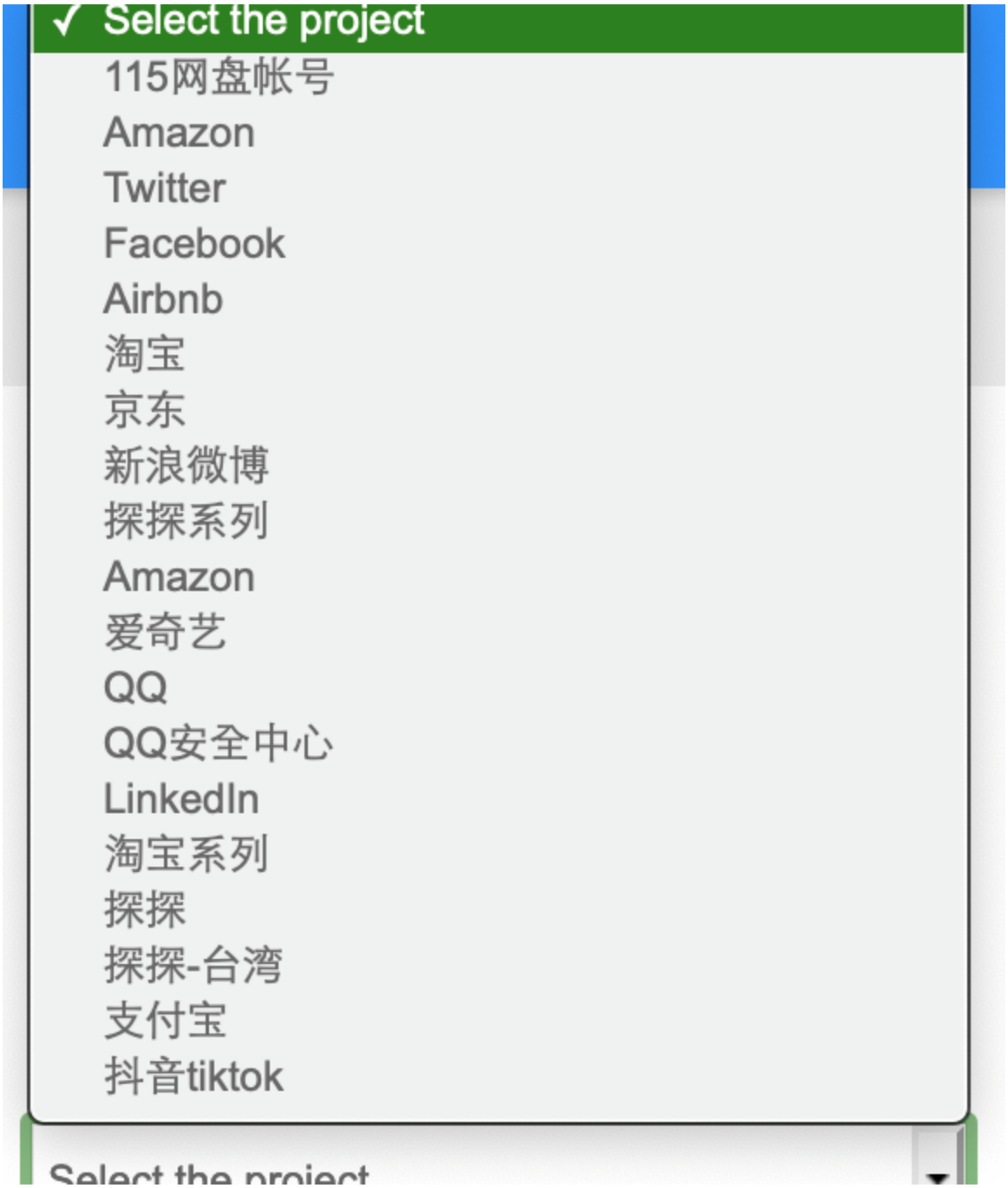
SMS PVA Services' Use of Infected Android Phones Reveals Flaws in SMS Verification

trendmicro.com/en_us/research/22/b/sms-pva-services-use-of-infected-android-phones-reveals-flaws-in-sms-verification.html

February 16, 2022



Using these code snippets and C&C traffic as fingerprints, we were able to identify two more DEX files with the same functionality but different C&Cs, indicating an active development process and several versions of both the development code and production code of the

Android malware.

Only text messages sent by specific services and matched by the regex provided by the C&C were intercepted. This is likely to prevent the user of the Android phone from discovering the malicious activity. The malware remains low-profile, collecting only the text messages that match the requested application so that it can covertly continue this activity for long periods. If the SMS PVA service allows its customers to access all messages on the infected phones, the owners would quickly notice the problem.

The SMS PVA service also controls the type of platforms that customers can receive text messages on (as listed in Figure 1). This means that the operators behind the service can make sure no obvious malicious activity occurs on the infected phones. If the service, for example, allowed the theft of two-factor authentication (2FA) for banking apps, then the real users would be alerted and take action, which would then result in the SMS PVA service losing its asset.

Use of residential proxies

Online platforms and services often authenticate new accounts by validating the location of the user during registration. For example, an IP address might be required to match the geographical location of the phone number used for the account.

To circumvent this, SMS PVA users use third-party IP masking services, such as proxies or virtual private networks (VPNs), to change the IP address that will be recorded when they try to connect to a desired service. Using Trend Micro™ Smart Protection Network™ (SPN) telemetry, we have identified that the users of SMS PVA services extensively use a variety of proxy services and distributed VPN platforms to bypass the IP geolocation verification checks.

User registration requests and SMS PVA API requests often come from an exit node of a VPN service or a residential proxy system. This means that the users of SMS PVA services typically use them in combination with some sort of residential proxy or a VPN service that allows them to select the country of the IP exit node to match the telephone number used to register the service.

Security implications of SMS PVA services and their effects on SMS verification

SMS verification has become the default authentication method for many online platforms and applications. Many IT departments treat SMS verification as a “secure” black box validation tool for user accounts. Currently, however, online services and platforms should be wary about heavily relying on SMS verification. These SMS PVA services prove that cybercriminals are indeed able to defeat SMS verification at scale. This also means that there could be authenticated and verified accounts on platforms that behave like bots, trolls, or fraudulent accounts.

"Authentic user behavior" on certain platforms can be manipulated by malicious actors with SMS PVA accounts. This means that a platform could incur increased costs due to scam and fraud. A platform might even be involved (directly or indirectly) with personal injury or damage to property.

Based on previous uses of fake accounts, we can predict how threat actors will use these services in their scams and criminal activities.

Anonymity tool

Cybercriminals use disposable numbers for many different activities because they can register accounts without worrying about being traced. Also, because the infected mobile phone numbers they use are attached to real people, law enforcement inquests about their accounts will be traced to another person.

We saw one example of misuse linked to a buy-now-pay-later scheme. In this example, several malware samples used SMS PVA services to acquire phone numbers and linked those numbers to existing online payment service accounts. Afterward, the malicious actors attempted purchase transactions from an online shopping site. Although we only identified a few samples of such activities, we believe that when automated, these accounts can be used at large to perform illicit purchases or money laundering.

These services can also be used to avoid responsibility for damages or illegal activity on commerce platforms. In 2020, a Russian car-sharing service accused a man of being involved in a car accident. However, it was revealed that the account used for the car-sharing service was a fraudulent account set up using the accused man's name and disposable SIM cards for verification.

Coordinated inauthentic behavior

Coordinated inauthentic behavior is often used to distribute and amplify information (often misinformation) in social networks. This can be done at scale, fast, and with the necessary speed and precision using SMS PVA services. Large campaigns can be used to manipulate public opinion on brands, services, political views, or government programs such as vaccination campaigns. Organizers of fake news can even use SMS PVA services to create online troll armies.

Some SMS PVA services have thousands of compromised smartphones spread across various countries. The service can allow customers to register social media accounts in bulk and in specific countries that the actors behind these services are targeting.

Abuse of sign-on bonuses

Sign-on bonuses (often given whenever a new account is registered) can also be abused using the SMS PVA service. For example, Bolt, a ride-hailing service popular in Eastern Europe, Africa, and Western Asia, incentivized new sign-ons by giving away free ride credits for every new account. Some SMS PVA services realized this as a potential monetization scheme and even advertised having "unlimited discounted Bolt rides" to persuade people to use the SMS PVA service.

Conclusions and recommendations

The core security issue is that an enterprise has the ability to monitor and intercept text messaging from tens of thousands of devices all around the world, and then profit from this interception by offering the service to whoever can pay for it. Another chilling thought is that the customizable regular expression patterns supplied by the C&C mean that the SMS interception capability is not limited to verification codes. It can also be extended to the collection of one-time password (OTP) tokens or even used as a monitoring tool by oppressive regimes.

The SMS PVA service operation not only shows the inadequacy and insufficiency of one-time SMS verification as the primary means of validation, but also highlights the need for better mobile security and privacy. The malware that infects these phones might be unwittingly downloaded by users, or could imply a gap in supply-chain security.

Trend Micro is able to detect the malicious code and block traffic to C&C servers. But a comprehensive solution requires challenging built-in fundamental assumptions with respect to account verification, more effective content moderation, and enhancing smartphone security.

To read more about this threat, download our research paper, "SMS PVA: An Underground Service Enabling Threat Actors to Register Bulk Fake Accounts."

Indicators of Compromise (IOCs)

Dex SHA 1	**Detection**
24b24990937b4265e276db8271b309c05e1d374b	AndroidOS_Guerrilla.HRXD
6a65e2a484f49e82a0cea5a1c2d5706314f0064a	AndroidOS_Guerrilla.HRXD
e83ec56dfb094fb87b57b67449d23a18208d3091	AndroidOS_Guerrilla.HRXD

Domains:

- **Smspva[.]net**
- **Enjoynut[.]cn**
- **Sublemontree[.]com**
- **Lemon91[.]com**

- **Lemon91[.]top**

Mobile

Certain SMS PVA services allow their customers to create disposable user profiles or register multiple accounts on many popular online platforms. These services can be abused by criminals to conduct fraud or other malicious activities.

By: Zhengyu Dong, Ryan Flores, Vladimir Kropotov, Paul Pajares, Fyodor Yarochkin
February 16, 2022 Read time: (words)