Android trojan TgToxic updates its capabilities

intel471.com/blog/android-trojan-tgtoxic-updates-its-capabilities

TgToxic is an Android banking trojan discovered by Trend Micro in July 2022. It's designed to steal user credentials, cryptocurrency from digital wallets and funds from banking and finance apps. It initially was observed targeting mobile users in Southeast Asia through social-engineering campaigns, distributing malware samples via phishing sites and deceptive applications that mimic legitimate services such as government assistance websites. Additionally, malware was promoted through compromised social media accounts and third-party platforms, often under the guise of dating, messaging or financial applications.

In October 2024, researchers with online fraud management software provider Cleafy published an article about a new version of TgToxic malware, which they called the ToxicPanda strain. Their analysis revealed this version still was under development, evident from several unimplemented commands and a general reduction in technical sophistication compared to its predecessor. Additionally, the report pointed to suspected plans by the malware operators to expand their geographical reach. This expansion is evidenced by the inclusion of European and Latin American banks in the list of targeted applications, indicating a potential broadening of their operational focus to encompass additional regions.

On Nov. 22, 2024, Intel 471 mobile malware researchers observed a campaign leveraging an updated version of TgToxic. We believe these updates could be a direct response to the detailed blog post published by Cleafy which exposed the functionality of the newer TgToxic version. This new version of the trojan abused 25 community forums to host encrypted malware configurations. The actors created user accounts on these forums and embedded specific encrypted strings within the user profiles, serving as dead drop locations from which malware bots could retrieve the final command-and-control (C2) URL.

However, this second version was only in use for a few weeks before being replaced by a third variant, which is still being leveraged by the threat actors at the time of this report. The actors once again changed the way the malware obtains the C2 URL, from a dead drop location to a domain generation algorithm (DGA). This shift may have been triggered by the reporting and subsequent removal of the dead drop accounts from various forums.

The modifications seen in the TgToxic payloads reflect the actors' ongoing surveillance of open source intelligence and demonstrate their commitment to enhancing the malware's capabilities to improve security measures and keep researchers at bay. This blog post will discuss specifics of the campaign and the malware updates.

The campaign

The samples associated with the campaign were hosted on the open directory at the mta164.bwhite.com website. We suspect these samples may have been delivered through short message service (SMS) texts, phishing websites or deceptive applications; however, we currently lack direct evidence confirming the specific methods used for their delivery.

This image depicts the open directory that hosted both the dropper and main payload involved in the campaign Nov. 26, 2024.

Two Android application package (APK) samples are within the open directory. The sample labeled “dropper.apk” is part of the TiramisuDropper malware family, functioning as a loader to facilitate the installation of the final “no_dropper.apk” payload. In this case, the final payload is an updated version of TgToxic.

Version updates

Analysis of the latest version of the malware revealed several changes, including improved emulator detection capabilities and updates to the C2 URL generation mechanism, as detailed below.

Improved emulator detection capabilities. The latest samples of TgToxic were enhanced with multiple anti-emulation techniques to circumvent automated analysis systems. These techniques incorporate a multifaceted approach to system verification. Key methods include:

Android system features check and hardware fingerprinting. The malware conducts a thorough evaluation of the device’s hardware and system capabilities to detect emulation. It assesses crucial Android system features typically absent in emulators, such as Bluetooth capabilities, sensor availability and telephony services. The malware concurrently scrutinizes the central processing unit (CPU) architecture to determine whether it is running on processors commonly supported by emulators, such as AMD or Intel processors.

```
try {
Process process0 = new ProcessBuilder(new String[]{"/system/bin/cat", "/proc/cpuinfo"}).start();
StringBuffer stringBuffer0 = new StringBuffer();
BufferedReader bufferedReader0 = new BufferedReader(new InputStreamReader(process0.getInputStream(), "utf-8"));
String s6;
while((s6 = bufferedReader0.readLine()) != null) {
     stringBuffer0.append(s6);
}

bufferedReader0.close();
s = stringBuffer0.toString().toLowerCase();
....

if(!s.contains("intel") && !s.contains("amd")) {
BluetoothAdapter bluetoothAdapter0 = BluetoothAdapter.getDefaultAdapter();
if(bluetoothAdapter0 == null) {
     return true;
}

return UOOOIIOI:(context0, "android.permission.BLUETOOTH_CONNECT") == 0 && TextUtils.isEmpty(bluetoothAdapter0.getName()) ? true
}
```

The image depicts the emulator detection routine through hardware fingerprinting in the new TgToxic versions Nov. 26, 2024.

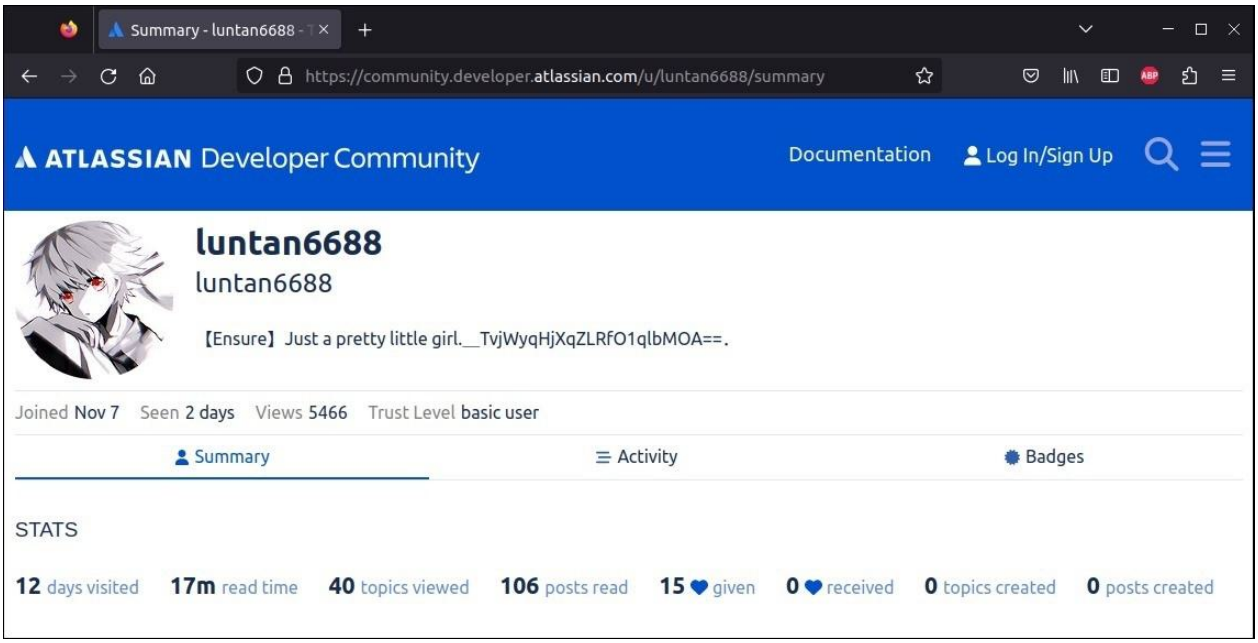
System property analysis and emulator-specific indicators. The malware examines a set of device properties including brand, model, manufacturer and fingerprint values to identify discrepancies that are typical of emulated systems. It simultaneously searches for direct indicators of emulation, such as the presence of Quick Emulator (QEMU), an open source emulator and virtualization software used for running various operating systems on different processor architectures, and Genymotion, a specialized Android emulator that simulates Android devices for development and testing. It also detects generic hardware signatures, test keys and emulator names such as the "google_sdk" or "vbox86p" products.

```
if(Build.FINGERPRINT.startsWith("generic") ||
   Build.FINGERPRINT.toLowerCase().contains("vbox") ||
   Build.FINGERPRINT.toLowerCase().contains("test-keys") ||
   (Build.MODEL.contains("google_sdk") ||
   Build.MODEL.contains("Emulator") ||
   Build.MODEL.contains("Android SDK built for x86")) ||
   (Build.MANUFACTURER.contains("Genymotion") ||
   Build.MANUFACTURER.equals("unknown") ||
   ((TelephonyManager)context0.getSystemService("phone")).getNetworkOperatorName().equalsIgnoreCase("android"))) {
return true;
}

String s2 = Build.PRODUCT;
if(s2 == null) {
return true;
}

if(!s2.equals("sdk") && !s2.equals("sdk_x86") && !s2.equals("google_sdk") && !s2.equals("vbox86p") && !s2.equals("emulator")) {
String s3 = Build.BOARD;
if(s3 == null) {
     return true;
}
```

The image depicts the emulator detection routine through device build properties in the new TgToxic versions Nov. 26, 2024.

Updates from hard-coded C2 to dead drop locations

Previous versions of TgToxic featured hard-coded C2 domains and subdomains in the malware configuration. However, the second variant has shifted to using a set of URLs that direct to the specific “luntan6688” username on forums hosted by 25 different companies. Visiting the profile page of this user on any of the listed forums reveals the actors included an encrypted string following the “Just a pretty little girl.__” delimiter.



The image depicts the luntan6688 user profile on the Atlassian community developer forum Nov. 26, 2024.

To generate the C2 URL from a dead drop location, the malware randomly selects a community forum URL from those embedded in its configuration, then parses the hypertext markup language (HTML) content on the page. To retrieve the encrypted string, the malware splits the page content at the "_" delimiter and iterates through the resulting segments, identifying and retrieving the encrypted section by searching for the segment that contains the full stop character.

For decryption, TgToxic instances utilize the data encryption standard (DES) algorithm in cipher block chaining (CBC) mode and the PKCS5Padding scheme. Across all observed samples, the string “jp202411” consistently is used as both the encryption key and the initialization vector.

In the specific case illustrated in Figure 4, the C2 derived from the dead drop location is sakiwmk.top, leading the malware to establish connection to https://ctrl.sakiwmk.top. Once the correct C2 connection is established, malware operators can use the infected device to perpetrate fraud and control it.

Threat actors derive several advantages from using public services to host malware configurations. First, they avoid the costs associated with maintaining their own infrastructure. Second, they exploit the perceived legitimacy of community forums to bypass security measures. Moreover, it is important to note that once a C2 server is deactivated or taken down, the associated malware sample becomes obsolete since it cannot connect to a new server without an updated address. However, by employing the dead drop technique — a strategy that is not new but remains popular among many threat actors — they simply can update the community user profile to point to a new C2 address. This method considerably extends the operational lifespan of malware samples, keeping them functional as long as the user profiles on these forums remain active.

Switch to DGA

Starting from the beginning of December 2024, Intel 471 mobile malware researchers identified a third variant of TgToxic using a DGA to periodically generate new domain names used as C2 servers. Some of the top-level domains (TLDs) are in the figure below.

```
CLS2868.FLD26996 = new String[]{"com", "net", "org", "edu", "info", "top", "club",
        "help", "click", "biz", "sbs", "xyz", "lat", "cfd", "one", "icu", "de", "lol", "buzz", "rest",
        "in", "us", "online", "run", "bond", "pics", "fun", "best", "uk", "me", "website", "site",
        "life", "art", "media", "uno", "store", "email", "bar", "nl", "vin", "reisen", "golf", "zone",
        "wine", "kaufen", "gold", "rocks", "dog", "delivery", "sale", "republican", "cheap", "live",
        "link", "do", "tires", "education", "blog", "community", "company", "network", "cc", "vip",
        "college", "pro", "mobi", "name", "web", "app", "tech", "travel", "shop", "post", "fm",
        "asia", "coop"};
```

The image depicts the TLDs included in the malware configuration Feb. 14, 2025.

The reason for this further change lies in the several advantages of using a DGA. Unlike hard-coded C2 server addresses, which can be easily identified and blocked by security systems, DGAs dynamically generate multiple domain names, making it harder for defenders to track and disrupt communications. This technique increases the resilience of the malware, as even if some domains are taken down, malware operators can quickly switch to new ones. In fact, TgToxic instances try to connect sequentially to each domain starting from the ".com" TLD until it can establish a connection to one of the generated domains.

Assessment

The recent updates to the TgToxic malware are noteworthy, highlighting both continuous improvement and a deliberate expansion of its operational scope by its operators. This effort to broaden the malware's reach suggests a calculated attempt to engage new markets and demographic groups beyond its original targets in Southeast Asia.

Moreover, it is crucial to recognize the actors behind TgToxic actively monitor open source intelligence and adjust their strategies accordingly. This ongoing surveillance of the cybersecurity landscape enables them to make timely decisions and modify their tactics to circumvent new security defenses effectively. This proactive stance poses significant challenges for defense strategies and underscores the need for dynamic, adaptive cybersecurity measures to counter these evolving threats effectively.

Recommendations

Prevention strategies

Restrict app installations: Disable the settings option "Allow from Unknown Sources" on Android devices to prevent installation of APKs from unauthorized sources. In corporate environments, only install APKs from official app stores and further restrict this to a list of preapproved apps to minimize risks.

Leverage mobile device management: Consider deploying mobile device management (MDM) software to enhance corporate security on smartphones, tablets and other portable devices used within an organization.

Use mobile threat defense: Deploy a mobile threat defense software to monitor and manage traffic directly on devices. This is crucial, since portable devices often escape the security controls of traditional local networks.

Monitor permissions requests: Be vigilant of apps that request excessive permissions. Pay special attention to any app requesting "Accessibility services permission," since this frequently is exploited in fraud-oriented applications.

Deploy indicators of compromise: Consider deploying the indicators of compromise (IoCs) available in Titan for timely detection of potential threats.

Perform regular cybersecurity training: Provide ongoing cybersecurity training for all staff members. Emphasize the importance of recognizing phishing and malicious SMS messages prompting users to install applications.

MITRE ATT&CK techniques

Technique Title	ID	Use
Initial Access [TA0027]		
Phishing: SMS phishing messages	T1566.001	Attackers send SMS messages to lure victims into downloading malicious application from a link
Defense Evasion [TA0030]		
Sandbox Evasion: System Checks	T1633.001	TgToxic checks different system properties to detect a virtual environment
Masquerading: Match Legitimate Name	T1655.001	TgToxic samples masquerade as the legitimate Google Chrome application
Credential Access [TA0031]		
Input Capture: Keylogging	T1417.001	TgToxic instances collect sensitive information such as login credentials through keylogging
Command and Control [TA0037]		
Web Service: Dead Drop Resolver	T1481.001	Attackers leverage community forums to host the encrypted malware configuration
Non-Standard Port	T1509	TgToxic instances start communications with the C2 using HTTPS requests over port 443. The C2 response then instructs to switch communications over to websockets using a particular port included in the response
Encrypted Channel: Symmetric Cryptography	T1521.001	Attackers encrypt the malware communications using the AES algorithm in ECB mode with the PKCS5Padding padding scheme
Dynamic Resolution: Domain Generation Algorithms	T1637.001	TgToxic instances use Domain Generation Algorithms to connect to the C2 server.

This report comes from Intel 471's Malware Intelligence team, which tracks and collects indicators and artifacts from more than 300 malware families and more than 60 mobile malware families. Malware Intelligence provides near-real time proactive insights into malware and related threat actor activity using the Technical Research & Analysis Platform (TRAP), our automated framework for tracking and monitoring malware. TRAP is further enhanced with near-real time surveillance of malware activity at the C2 level, providing deep insights and context into malware operations using our unique and patented Malware Emulation and Tracking System (METS). METS delivers near real-time insights and deep context in support of numerous cybersecurity and intelligence use cases.

For more information, please contact Intel 471.