CASE STUDY: BANKING TROJAN CAMPAIGN (2020)

OVERVIEW

In 2020, a widespread malware campaign leveraged banking trojans equipped with keylogger functionality to steal financial credentials from thousands of victims across multiple countries. Major trojans involved included Ursnif, TrickBot, and Cerberus, which targeted both Windows and Android devices. These attacks resulted in significant financial losses and highlighted the evolving sophistication of cyber threats to the global financial sector.

ATTACK VECTOR AND METHODOLOGY

1. Delivery Mechanisms

- The campaigns primarily used malicious spam emails containing infected attachments (such as Word or Excel files) or links to compromised websites. Once opened, these attachments executed the trojan payload on the victim's machine.
- On Android devices, trojans like Cerberus and EventBot disguised themselves as legitimate apps, often distributed through rogue app stores or phishing sites.

2. Infection and Execution

- Upon execution, the trojans installed themselves persistently on the victim's device.
- They requested extensive permissions (especially on mobile), including access to accessibility features, background operation, and SMS interception.

3. Keylogging and Credential Theft

- The core feature was a keylogger module that captured keystrokes, enabling the malware to record login credentials as users accessed online banking portals or financial apps.
- On Android, trojans exploited accessibility services to capture passwords, lockscreen PINs, and even OTPs sent via SMS.

4. Data Exfiltration

- Stolen credentials and sensitive data were transmitted in encrypted form to attacker-controlled servers.
- Some variants, like TrickBot, also harvested browser cookies, autofill data, and targeted cryptocurrency wallets.

SCALE AND IMPACT

- **Ursnif**: In May 2020, Ursnif surged in prevalence, entering the global top 10 malware list and doubling its impact on organizations worldwide. It targeted Windows PCs, stealing banking and email credentials through malicious spam campaigns.
- **Cerberus**: This Android banking trojan, active since 2019, was deployed in new campaigns using multi-stage droppers and Telegram bots for command and control. Cerberus leveraged keylogging, overlay attacks, and VNC to steal banking credentials and credit card details.
- **EventBot**: First identified in March 2020, EventBot targeted over 200 financial apps, using keylogging and SMS interception to bypass two-factor authentication and steal funds from bank accounts and crypto wallets.
- **TrickBot**: Widely used in 2020, TrickBot targeted financial services and businesses, stealing banking information, user credentials, and PII. It was also used to deploy additional malware or facilitate ransomware attacks.

GEOGRAPHIC REACH

- These campaigns affected victims in dozens of countries, with some trojans targeting hundreds of banks and financial institutions worldwide.

CONSEQUENCES

- **Financial Losses:** Victims suffered direct financial theft from compromised bank accounts and crypto wallets.

- **Credential Compromise:** Stolen credentials were sold or used for further fraud and identity theft.
- **Organizational Impact:** Many organizations faced data breaches, fraud, and regulatory scrutiny due to compromised employee and customer accounts.

NOTABLE TECHNIQUES

TROJAN	PLATFORM	KEY FEATURES	NOTEWORTHY TECHNIQUES
Ursnif	Windows	Keylogging, credential theft, persistence	Malicious spam, macro-laden docs
Cerberus	Android	Keylogging, overlay attacks, VNC, SMS theft	Fake apps, multi-stage droppers
EventBot	Android	Keylogging, accessibility abuse, SMS theft	Masquerades as legit apps
TrickBot	Windows	Keylogging, credential harvesting, lateral movement	Email phishing, module-based attacks

LESSONS LEARNED

- **User Awareness:** Phishing remains the primary delivery vector; ongoing user education is critical.
- **Multi-Factor Authentication:** Reduces risk but can be bypassed by advanced malware capable of intercepting OTPs.
- **Endpoint Security:** Regular updates, anti-malware solutions, and monitoring for suspicious activity are essential.
- **App Store Hygiene:** Only install apps from trusted sources, especially on mobile devices.

CONCLUSION

The 2020 banking trojan campaign demonstrated the global scale and sophistication of modern financial malware. By integrating keyloggers into banking trojans, attackers efficiently harvested credentials and bypassed security controls, affecting thousands of victims across multiple continents. This wave of attacks underscored the need for layered defenses, vigilant user behavior, and rapid response to evolving cyber threats.