Trellix

TLP:GREEN

THREAT LANDSCAPE REPORT

Banking/Financial/ Wealth Management – United States

Date Timeframe: September 1 to November 30, 2024

Threat Intelligence Group
threatintelligenceservices@trellix.com

TLP:GREEN

Executive Summary

The United States accounted for 39% (210,201,121) of the 538 million malicious file detections between September 1st and November 30th, 2024, and observed 15% (30,601,574) of the United States detections in the banking/financial/wealth management sector. The threat actor with the most malicious detections during the timeframe was the Chinese advanced persistent threat (APT) group Dalbit. Detections for the Lazarus Group, APT32, the Gamaredon Group, and APT28 were also observed during the timeframe and within the sector.

Contents

Introduction

This report provides a sampling of the threat landscape for the United States' banking sector through Trellix's repository of malicious detections. Trellix data catalogs banking with financial and wealth management and, as such, will be referred to as a singular sector – banking/financial/wealth management. The report will start with a global view, then move to a regional perspective, and finally end with the report's topic. It will highlight the malicious detections, top threat actors, and malicious files for the country's sector from September 1st to November 30th, 2024. In addition, open-source intelligence (OSINT) resources were utilized to provide additional threat actor and file details.

Report Considerations

The telemetry data in this report is strictly focused on malicious file detections. However, most of the information can be replicated through Trellix's malicious IP and URL detections.

In addition, the malicious detections are derived from Trellix products. The detection data offers valuable insights into the current cybersecurity threat landscape; however, it should not be considered a complete picture of all threats to a country or sector.

Global Detections

From September 1st to November 30th, Trellix telemetry observed 538,248,433 malicious file detections globally, including 82,742,640 in the banking/financial/wealth management sector, which ranked first globally. Next was government, followed by manufacturing, services, and healthcare.

The banking/financial/wealth management sector's most malicious detections occurred in the United States, accounting for 37% of all detections. Second was Australia, at 23%, followed by Brazil (9%), Indonesia (7%), and the Philippines (3%). See Figure 1 for the visualization sectors and top countries.

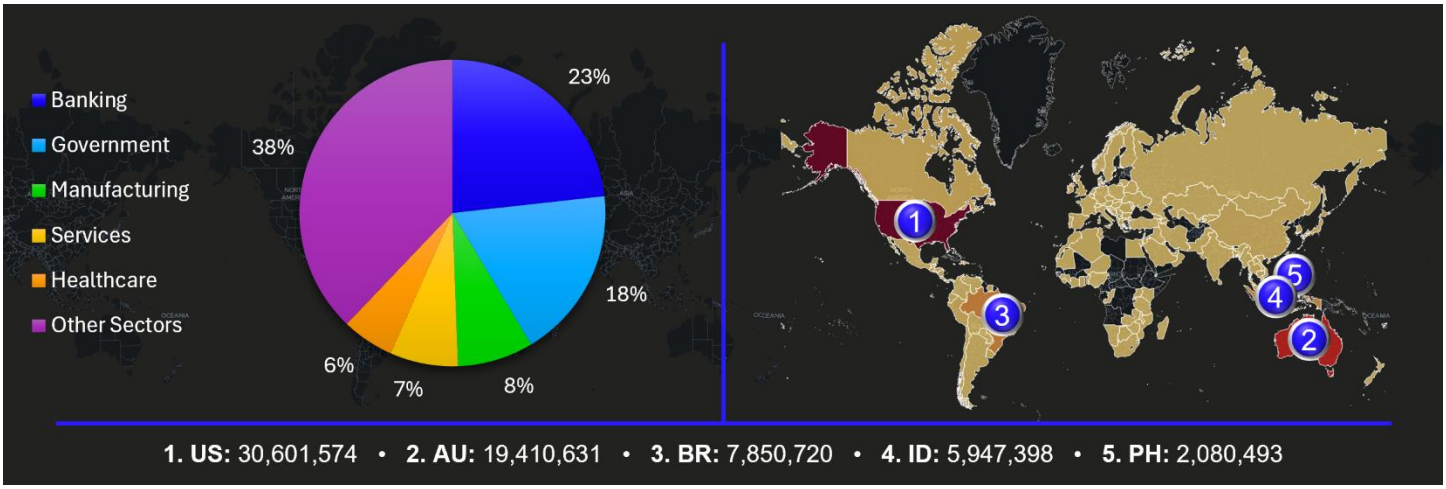


Figure 1. Top sectors globally and top countries for banking/financial/wealth management.

The Sandworm Team was the top threat actor for global malicious file detections in the banking/financial/wealth management sector. They accounted for 45% of the top five threat actor detections. APT29 followed them at 14%. Next was the RansomHUB Group (14%), APT40 (14%), and the Lazarus Group (12%). See Figure 2 for the global top threat actors.

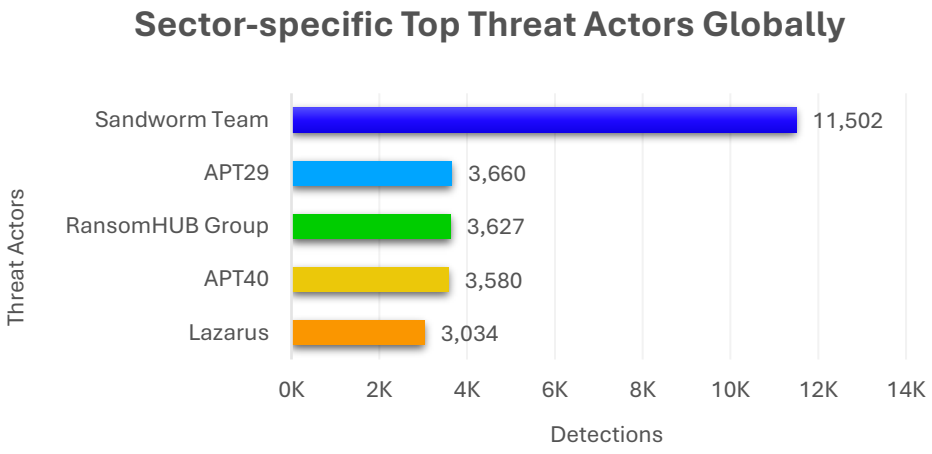


Figure 2. Top threat actors for the banking/financial/wealth management sector globally.

The Sandworm Team is believed to be affiliated with Russia's military intelligence agency, the GRU. Since 2009, they have been known for their sophisticated and adaptable tactics, techniques, and procedures (TTPs). The group targets critical infrastructure organizations, government entities, and media outlets, with a particular focus on Ukraine. Sandworm's activities include cyber espionage, disruptive attacks, influence campaigns, and data theft. Their motivations have primarily been to serve Russia's strategic and political goals[1]

North America (NA) Detections

Of the 82 million malicious file detections in the banking/financial/wealth management sector, 31,912,555 occurred within Canada and the United States.

The banking/financial/wealth management sector had the second-most detections in NA. First was government, with healthcare third. Next were Services and manufacturing. See Figure 3 for the top sectors and visualization of NA's top countries for banking/financial/wealth management.

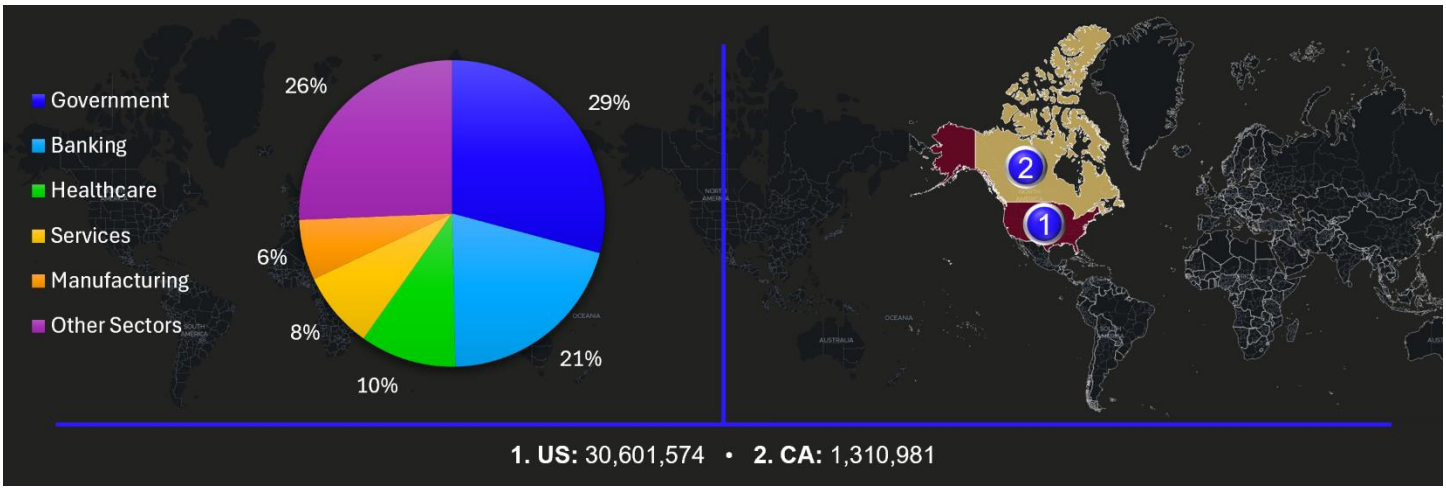


Figure 3. Top sectors in NA and top countries for banking/financial/wealth management.

Dalbit was also the top threat actor for malicious file detections in NA's banking/financial/wealth management sector. The group accounted for 7% of all threat actor detections in the region. The Sandworm Team followed them at 6%. Next were APT29 (6%), the Lazarus Group (4%), and the DarkSide Group (4%). See Figure 4 for the NA's top threat actors.

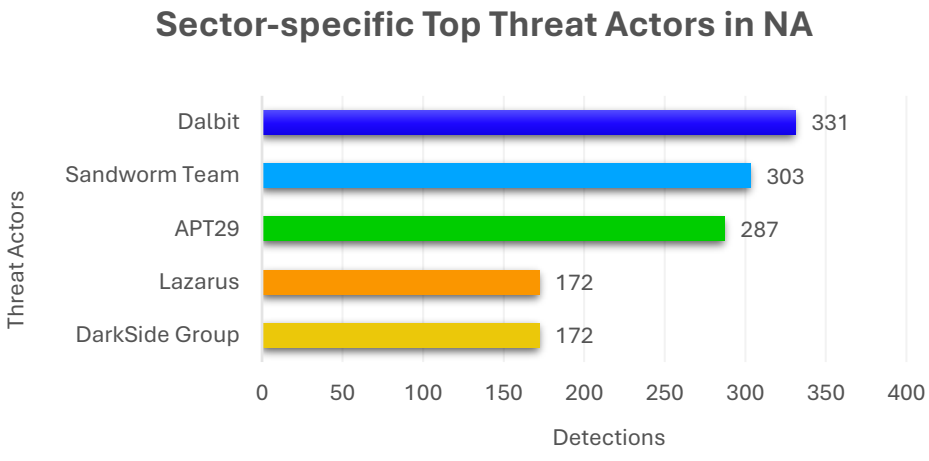


Figure 4. Top threat actors for the banking/financial/wealth management sector in NA.

Dalbit, also known as m00nlight, is identified as a nation-state-sponsored threat actor associated with Chinese cyber operations. Dalbit is involved in cyber espionage and other malicious activities targeting various sectors, including healthcare and software. Their operations often align with the broader objectives of Chinese intelligence efforts, making them a significant player in the landscape of cyber threats attributed to China.[2]

United States Detections

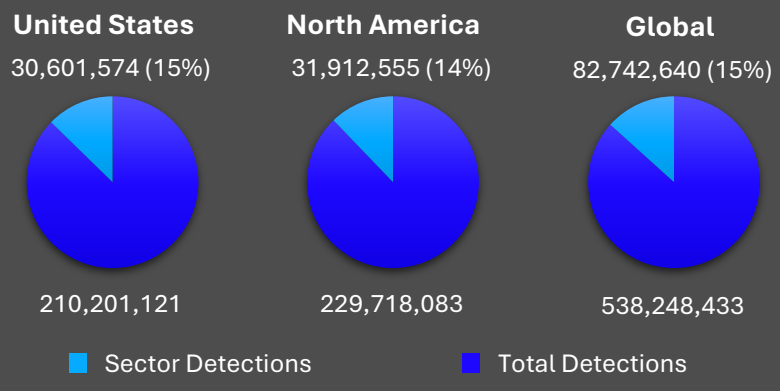
The United States accounted for 39% (210,201,121) of the 538 million malicious file detections between September 1st and November 30th and observed 15% (30,601,574) of the United States detections in the banking/financial/wealth management sector.

Like the NA detections, the banking/financial/wealth management sector was second among all sectors in the country. The government sector came first, with healthcare at third. Next were technology/IT and manufacturing.

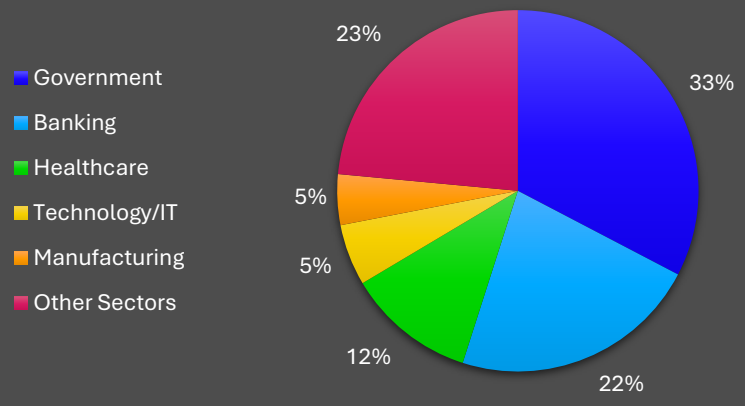
Dalbit was also the top threat actor in the United States, accounting for 17% of all threat actor malicious detections in the banking/financial/wealth management sector.

Dalbit, also known as m00nlight, is identified as a nation-state-sponsored threat actor associated with Chinese cyber operations. Dalbit is involved in cyber espionage and other malicious activities targeting various sectors, including healthcare and software. They employ multiple tools and techniques, such as the Godzilla Webshell, ASPXSpy, BlueShell, CHINACHOPPER, Cobalt Strike, Ladon, MimiKatz, and others. They have targeted web services of Korean corporations and are associated with other APT groups like Melofee, PingPull, SoWaT, Sword2033, MgBot, MQsTTang, PlugX, TONESHELL, and MirrorFace. Their operations often align with the broader objectives of Chinese intelligence efforts, making them a significant player in the landscape of cyber threats attributed to China.[2]

Detections Comparison Between Locations



Top Sectors in the United States



Sector-specific Top Threat Actors in the United States

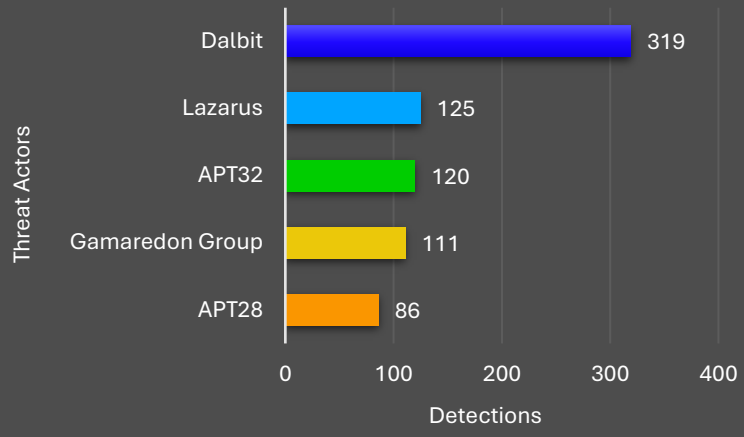


Table 1 provides the potentially malicious files associated with Dalbit within the banking/financial/wealth management sector in the United States. Table 2 focuses on the malicious files detected in the United States and the sector but unrelated to the top threat actors. Other vendors have also categorized these files as malicious. The Ratio column, provided by VirusTotal, annotates the number of malicious determinations over the total number of vendors. Along with Ratio, details from VirusTotal are annotated within the columns File Type and File Name. Trellix provides the GTI classification.

Table 1. Top malicious files for Dalbit observed in the banking/financial/wealth management sector.

MD5	GTI Classification	Ratio	File Type	File Name
46f366e3ee36c05ab5a7a319319f7c72	Trojan	63 / 72	Win32 EXE	mimikatz.exe
2ed0a868520c31e27e69a0ab1a4e690d	Trojan	36 / 64	ELF	rpcd
30fe6a0ba1d77e05a19d87fcf99e7ca5	Trojan	39 / 65	ELF	orbds
3f022d65129238c2d34e41deba3e24d3	Trojan	36 / 65	ELF	.ICECache
425c761a125b7cb674887121312bd16c	Trojan	34 / 65	ELF	/tmp/kthread

46f366e3ee36c05ab5a7a319319f7c72 has been linked to multiple attack vectors, including abuse of application functionality and privilege escalation, as well as being categorized under three malware families: Stealware, Backdoor, and Mimikatz. AESC released a report on February 13, 2023, that included this file. The report "Dalbit (m00nlight): Chinese Hacker Group’s APT Attack Campaign" discusses Dalbit's operation targeting Southeast Asian organizations, leveraging spear-phishing emails with malicious documents to infiltrate systems. The attackers employ custom malware and exploits to maintain persistence, exfiltrate data, and evade detection.[3]

Table 2. Top malicious files for the United States banking/financial/wealth management sector.

MD5s	
d29616351ef9a129027188527865b943	a36ca3de6b02c14693dc964a3b31e984
35fb9186949df8f348ade0f1f017acfa	1c9c5c41b2d05e348697411a5c93b1b5
7ccf5489f8c24c292a7a8969b8122065	253910caf90687c547748b100de29a6f
7dcc256c0ab5800fc8249c4f121f299b	4676ee761b3a36ceb38b9fa966900f4e
5ece1066ca9f48da57723ebcaf336074	15c761e4cad13b4275e535336d2196f7
bbd1e8c5cd49c08ec1e9d670d66b6c2c	b7eecc6d5963be7f077c1b10133f7c52
f336b3803be9f5b57d115c72aafa6d61	0f6e34932cfe4e5a0b8bdb11972a0732
038180710155fc18c82b0a2a00d41d8d	

Recommendations

Based on the malicious detections observed for this report, the Threat Intelligence Group provides the following recommendations.

Technical Controls

To bolster cybersecurity, organizations should implement robust file download monitoring and controls, deploy advanced endpoint detection and response (EDR) solutions, and enhance network segmentation to limit the potential lateral movement of threats. Strengthening authentication mechanisms and deploying application whitelisting can further protect systems by ensuring that only authorized users and applications can access critical resources.

Enhanced Monitoring

To enhance security, organizations should establish 24/7 monitoring with heightened scrutiny during high-risk periods, such as the last week of each month and end-of-quarter periods, where activity spikes have been identified. Automated alerting should also be implemented to detect unusual file download patterns, credential access attempts, and potential data exfiltration activities, enabling swift responses to suspicious behavior.

Security Awareness and Training

To strengthen security, organizations should conduct targeted phishing awareness training, provide regular security updates and briefings, and focus on educating employees about social engineering tactics. Staff should also be trained to identify suspicious file downloads, fostering a proactive approach to mitigating potential threats.

Strategic Security Measures

Organizations should review and update incident response plans, implement zero-trust architecture, and deploy network-based detection and response (NDR) systems to reinforce cybersecurity. Enhancing access control policies and conducting regular security assessments focusing on credential security, file download policies, network segmentation, and access controls are also critical to identifying vulnerabilities and mitigating risks.

Risk Mitigation Priorities

Organizations should prioritize protection against information-stealing tools to mitigate risks effectively, enforce strict download policies, and deploy advanced anti-phishing measures. Regular backup and recovery testing, coupled with enhanced monitoring of privileged accounts, ensures robust defenses against potential threats and minimizes the impact of security incidents.

Periodic Review and Updates

To maintain a strong security posture, organizations should conduct weekly security metrics reviews, monthly threat assessments, and quarterly updates to security controls. Regular penetration testing and continuous security posture assessments further ensure the effectiveness of defenses against evolving threats.

References

[1] Recorded Future – Sandworm Team Summary
[2] Recorded Future – Dalbit Summary
[3] https://asec.ahnlab.com/en/47455/