Global Cyber Threat Landscape Q2 2021

Key Industries Impacted, Prominent Threat Actors, Major Threats, and Mitigation Measures

Author: Hansika Saxena, Technical Writer, CloudSEK
Anandeshwar Unnikrishnan, Cyber Threat Analyst, CloudSEK

CloudSEK

Global Cyber Threat Landscape - Q2 2021

2021 has seen a variety of information security incidents as well as the rise in new attack vectors. We have put together data from XVigil and other sources to provide an overview of top global security incidents in Q2 2021.

Summary of Findings

Major Companies Targeted

- Amazon, Myntra & Swiggy (Bizongo)
- Upstox
- Apple
- Stanford University

Common Attack Vectors

- Phishing campaigns
- Exploitation of remote access solutions (VPN/RDP)
- Zero-day attacks
- Malvertising
- Ransomwares

Regions with Max. Incidents

- North America
- Europe
- Asia & Pacific
- Middle East
- South/Latin America
- Africa

Key Industries Impacted

- Finance & Banking
- E-commerce
- Service sector
- IT & Technology
- Media, Entertainment & Marketing

Threats to Finance Sector

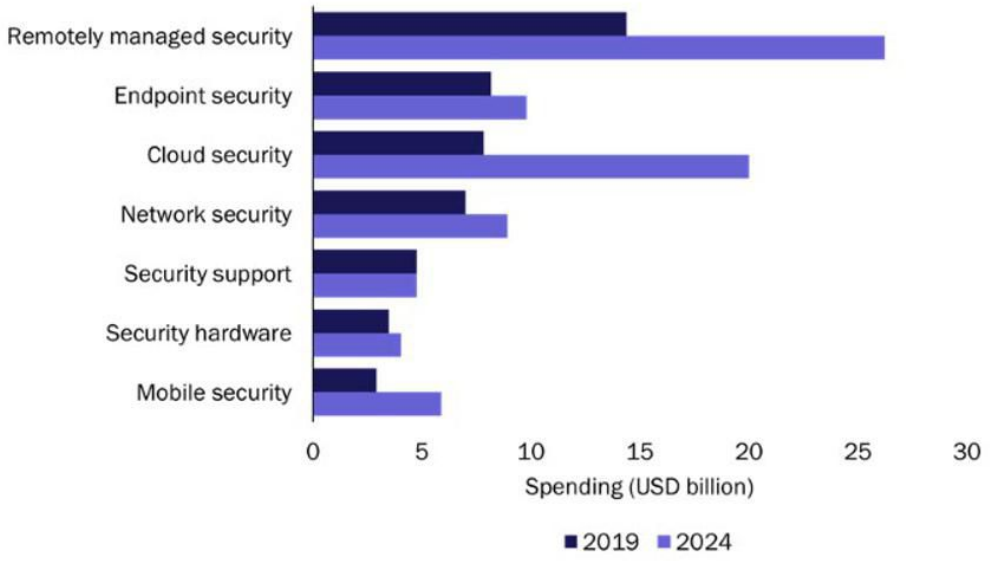
- Banking Trojans
- Ransomwares
- Distributed Denial of Service (DDoS)
- Business Email Compromise

Prominent Threat Actors

- Hacktivists
- Sponsored Threat Agents
- Inside Agents
- Cyber Terrorists
- Script Kiddies
- Organized Cybercriminals

Major Digital Threats of 2021

Last year (2020) saw rapid digital transformation across the globe. From remote working and online shopping to digital transactions and virtual socialization, there has been a paradigm shift in how we work, communicate, and collaborate. This has made organizations across sectors attractive targets for threat actors and sophisticated attack vectors. Big game hunters continued to target various industries, capitalizing on weak cybersecurity postures and significantly larger attack surfaces.



Spending predictions for SMBs for the next 4 years by Analysys Manson

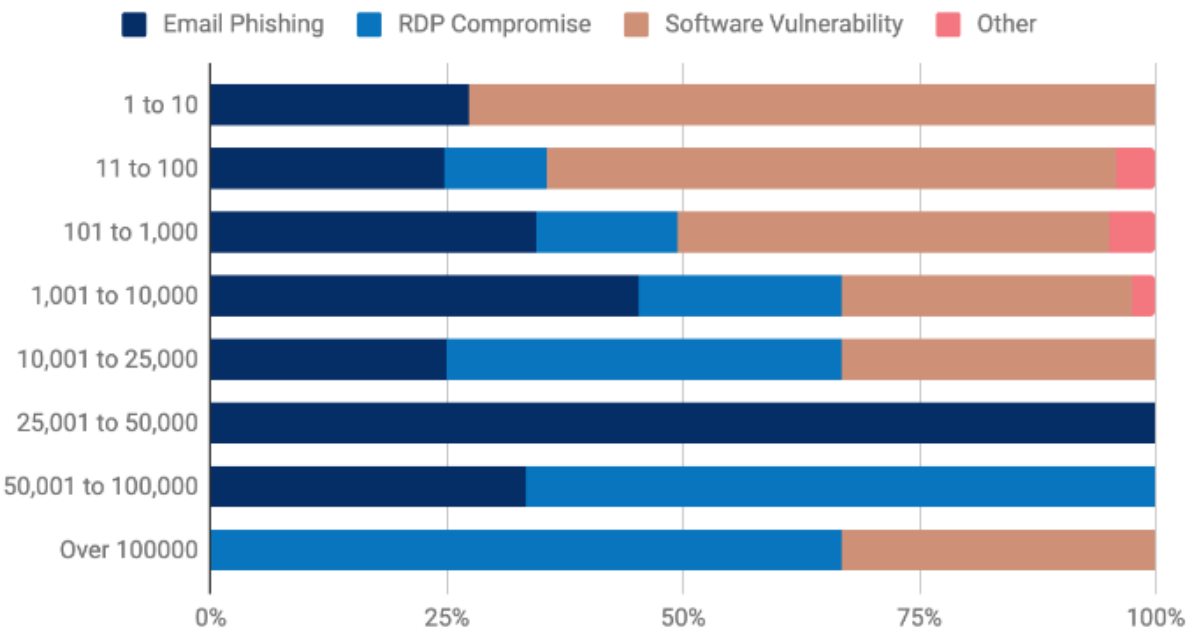
The most widely leveraged primary initial attack vector continues to be phishing campaigns. However, this year also saw a significant upward trend in the sophistication and scale of attacks. A large-scale impact was also achieved by exploiting remote access solutions such as VPN and RDP.

In a prediction made by Analysys Mason's SMB (Small and Medium-Sized Businesses) Technology Forecaster, it is anticipated that the annual SMB spending on cybersecurity worldwide will grow by 10% every year from 2019 onwards, and will reach almost USD 80 billion by 2024.

Common Attack Vectors

Our research shows that the most common attack vectors leveraged by threat actors to carry out cyberattacks include:

- Phishing campaigns
- Social engineering schemes
- Exploitation of remote access solutions such as VPN and RDP
- Zero-day attacks
- Malvertising: Malicious Advertising on social media, search engines, and SEO manipulation
- Ransomware attacks
- Business Email Compromise (BEC)
- Deepfakes and Identity threats

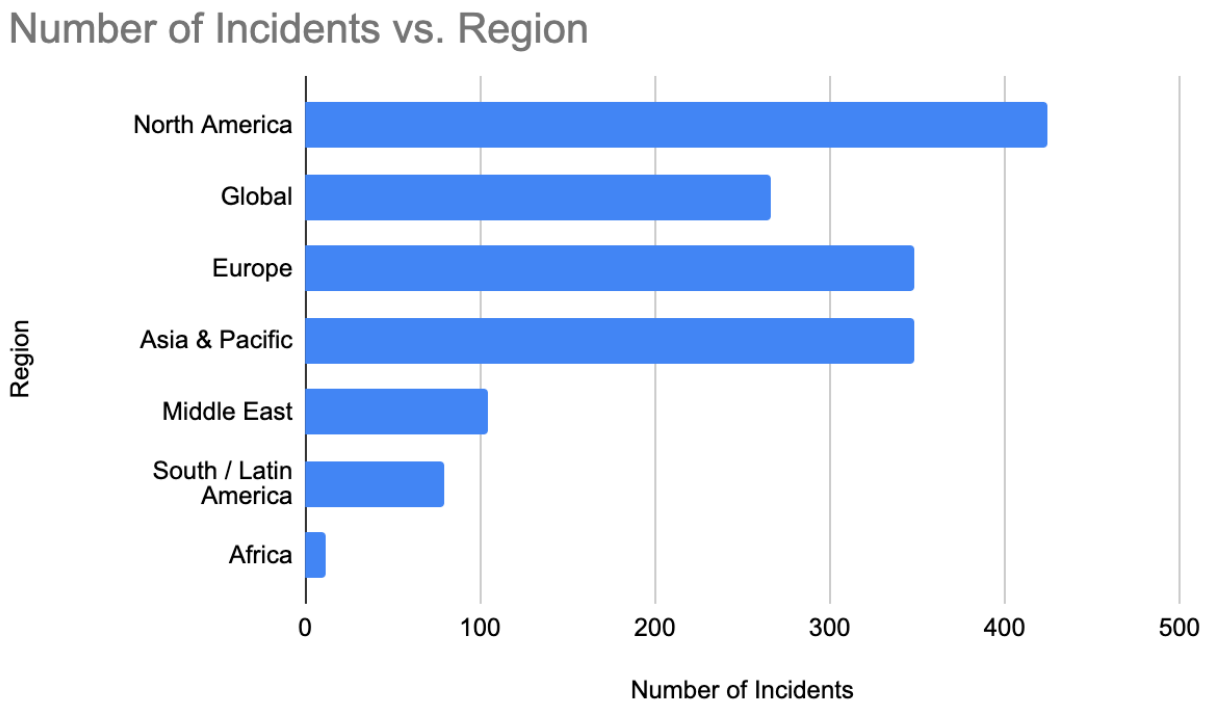


Common attack vectors used in 202 by company size via Coveware

It was observed that attack vectors vary according to the size of the targeted company. And despite the rise in new methods to breach a company, phishing attacks continue to be the most popular initial attack vector.

Most Targeted Regions

After analyzing the data gathered by XVigil, from multiple platforms across the internet in 2021, we found that the majority of cyber incidents targeted North America, followed by Europe, Asia, Pacific, Middle East, and Africa.

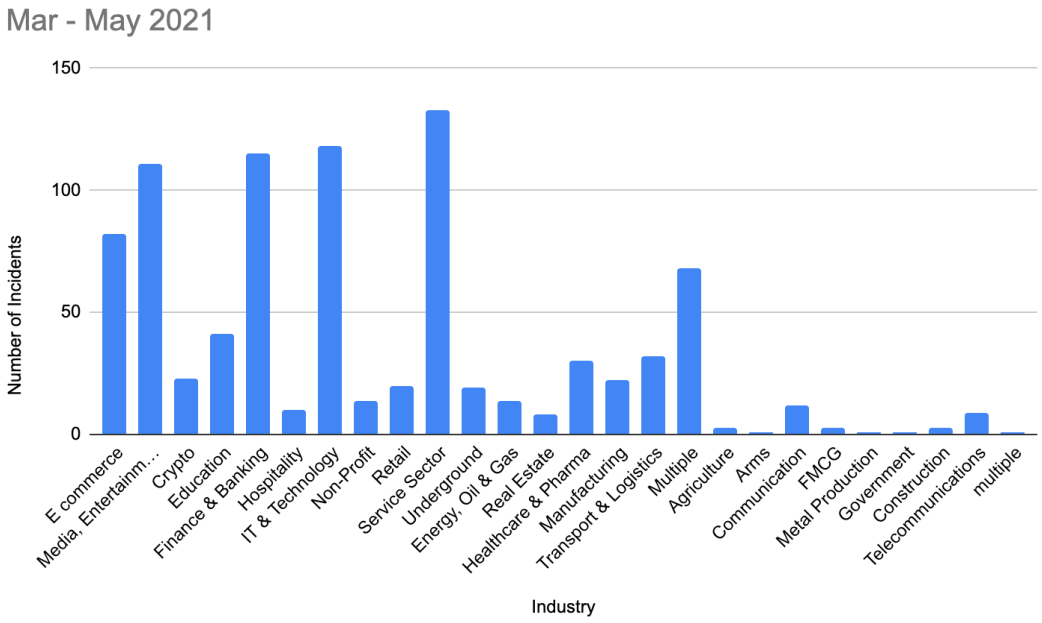


Number of attacks by the region affected

In 2020, India became the second most targeted country in the Asia Pacific region. Japan stood on the top of this list and these countries were closely followed by Australia. Finance and insurance were the most impacted sectors in India (60%), followed by manufacturing and professional services. Ransomware is the most prominent attack vector used, making up roughly 40% of attacks.

Key Industries Impacted

While a surge in cyber-attacks has affected the security posture of industries across every vertical, XVigil found that globally, the Service Sector was most commonly targeted by threat actors. The most targeted data types include access to organizations, customer databases, records acquired from credit card companies, malware, vulnerabilities, exploits, etc.



Number of incidents by the impacted industries

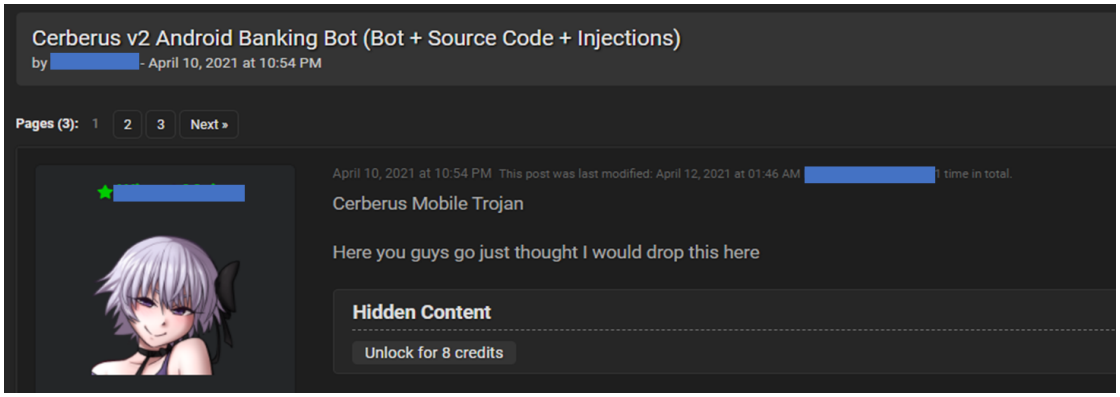
The top 5 impacted industries are:

Industry	No. of Incidents	High-profile Targets
Service Sector	133	Truecaller, Yellowpages, and a few job-hunting platforms
IT and Technology	118	Asus, Neoseeker, Tata, Nokia, Deloitte
Finance and Banking	115	Forex, Banco Pichincha Ecuador, American Express, FCI Bank, Upstox
Media, Entertainment, and Marketing	111	LinkedIn, Zee5, Facebook, Instagram, Tik Tok
E-commerce	88	Fossil, BigBasket, Indiamart, and other retail shops

Major Threats Targeting the Finance and Banking Sector

The finance and banking sector stood third in the top 5 industries impacted by threat actors. A variety of attack vectors were used to infiltrate organizations across the industry. Here are some of the major threats aimed at the sector:

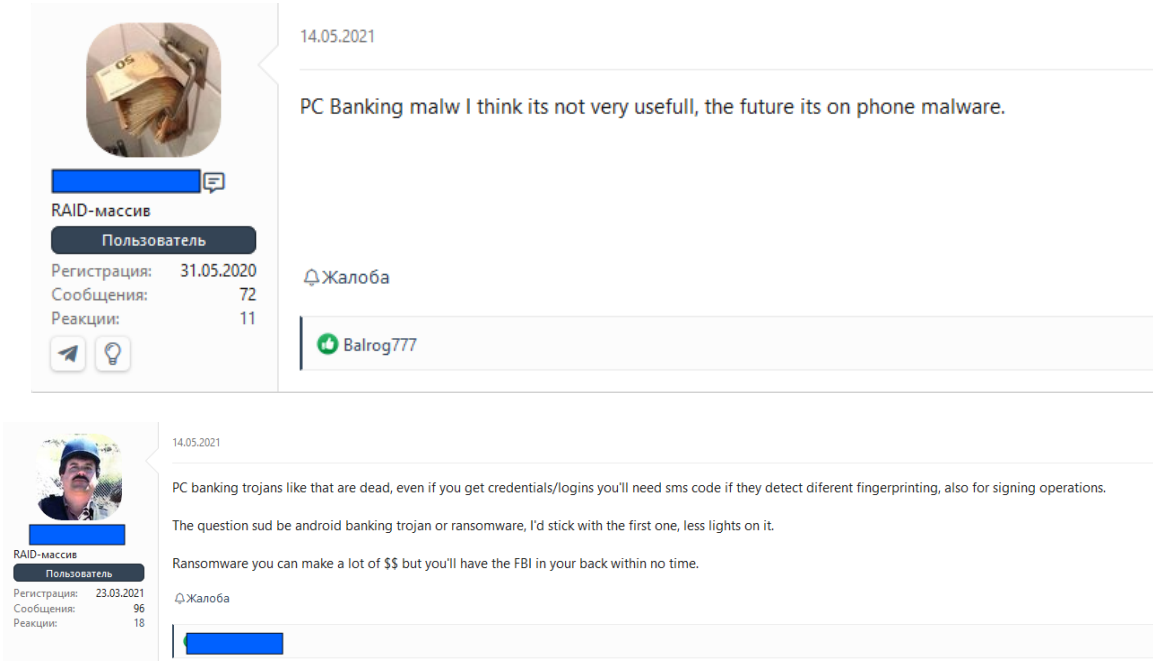
- **Banking Trojans**: Banking trojans are the most common vector used to target a bank's users. This allows threat actors to compromise a bank without targeting the bank's networks directly. Banking trojans target platforms such as Windows and Android. The functionality of a banking trojan is to steal banking credentials from compromised devices to make unauthorized transactions or to sell them on cybercrime forums.



Android banking trojan being shared on a cybercrime forum

- **Business Email Compromise (BEC):** also known as email account compromise (EAC) has been known as one of the most financially damaging online crimes. In this, cybercriminals spoof executive email addresses and request payments from large businesses, making it difficult to detect if an email is legitimate or not. This technique is largely used in combination with spear phishing and malware injections.

- **Ransomware & ATM Malware:** Ransomware has been a favored extortion tactic by malicious actors. ATM malware is a significant threat to banks since it doesn't require direct access to a bank's internal networks. Instead, they can be installed locally on vulnerable ATM machines. We have observed various threat actors advertising ATM malware across cybercrime forums.

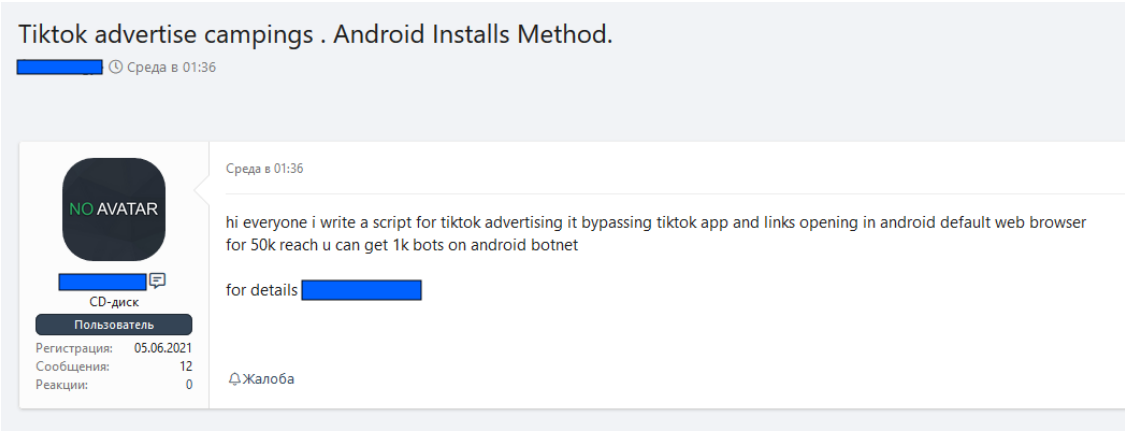


Underground chatter on malware

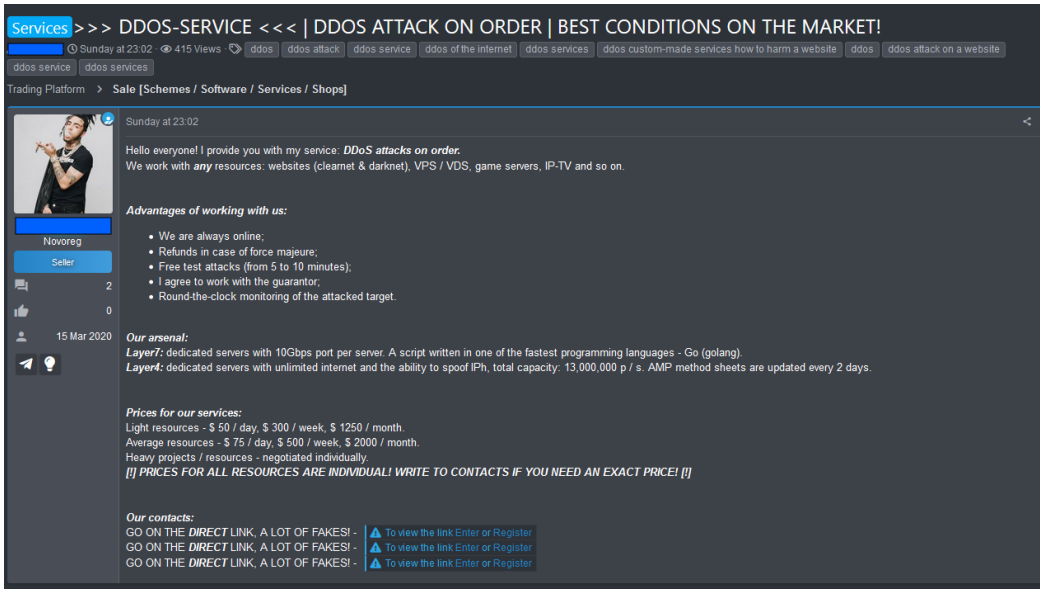
- **Supply Chain Vector -** State actors and financially motivated groups have started focusing on vendors who provide SaaS (Software as a Service) or other IT services, to launch attacks against their victims. The impact of supply chain compromise is far-reaching and provides more stealth for adversaries to infiltrate target networks where compromised vendor products and services are already whitelisted by security systems. Apart from vendors, infrastructure is also a hotspot for such malicious activities:
    - Vendor's **Continuous Integration & Continuous delivery [CI/CD] pipeline**.
    - Vendors cloud infra, specifically Kubernetes cluster and container technologies.
    - Vendor compromise use cases:
        - CodeCov breach 2021
        - Solar Winds/Sunburst 2020
        - Black Cocaine's attack on Nucleus Software Solutions

- **Network Attacks -** Adversaries infiltrate a bank's infrastructure and carry out reconnaissance to identify SWIFT terminals or servers that support ATMs. They then laterally move across the network to compromise these resources to perform unauthorized transactions.

- **Distributed Denial-of-Service (DDoS) -** DDoS attack is a cyber-attack in which the perpetrator seeks to make a machine or network resource unavailable to its intended users by temporarily or indefinitely disrupting services of a host connected to the Internet. DDoS attacks can also act as a cover for fraud, and are hence used in Mobile Banking Exploitation. In June 2020, the Internet Crime Complaint Center (IC3) published a Public Service Announcement warning that mobile banking usage has surged as much as 50%, which could lead to exploitation via app-based banking trojans and fake banking apps.



Threat actor claiming to offer 50K views via TikTok advertise campaign on a cybercrime forum



Post of DDoS service on a cybercrime forum

- **Indirect Vectors -** Threat actors are also known to use indirect attack vectors including:
    - Third-party vendor compromise

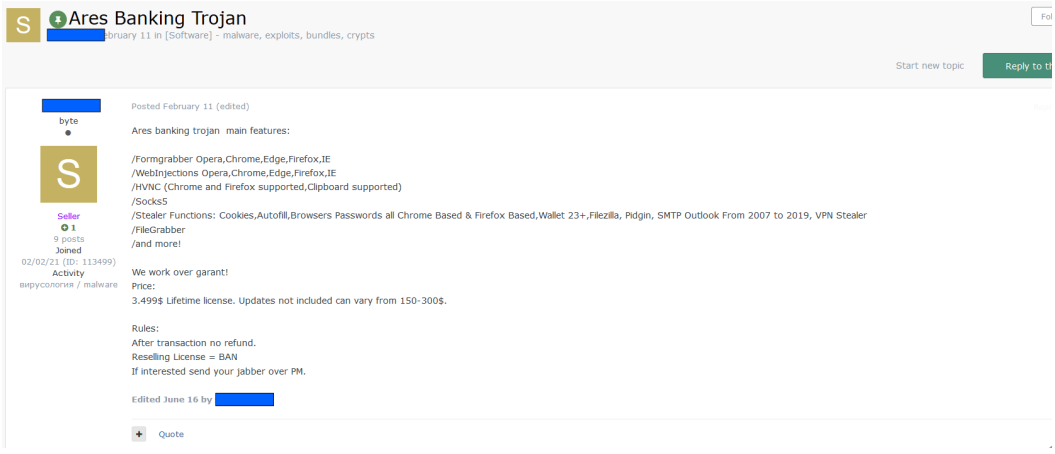
- Payment card data compromise
- Point-of-Sale (PoS) terminal attacks
- Phishing scams
- Online fraud

Mitigation Measures

Steps to Preempt Banking Trojans: Security products use known signatures and other heuristics data for behavioral detection to neutralize malware. However, if a malware's TTPs are sophisticated and new, security endpoints will have a hard time detecting them.

Here are some general guidelines:

- Create awareness among users.
- Be cautious while installing applications on mobile devices and install apps only from Google Play Store or Apple App Store and not from any untrusted third-party stores.
- Do not root your phone.
- Do not click on suspicious emails and messages.
- Use strong passwords and patterns and do not store them on your devices.
- Use Device administration API to set up password policy, remote wipe, etc.
- Update operating systems regularly.
- Use strong anti-virus.



Post on a Banking Trojan on a cybercrime forum

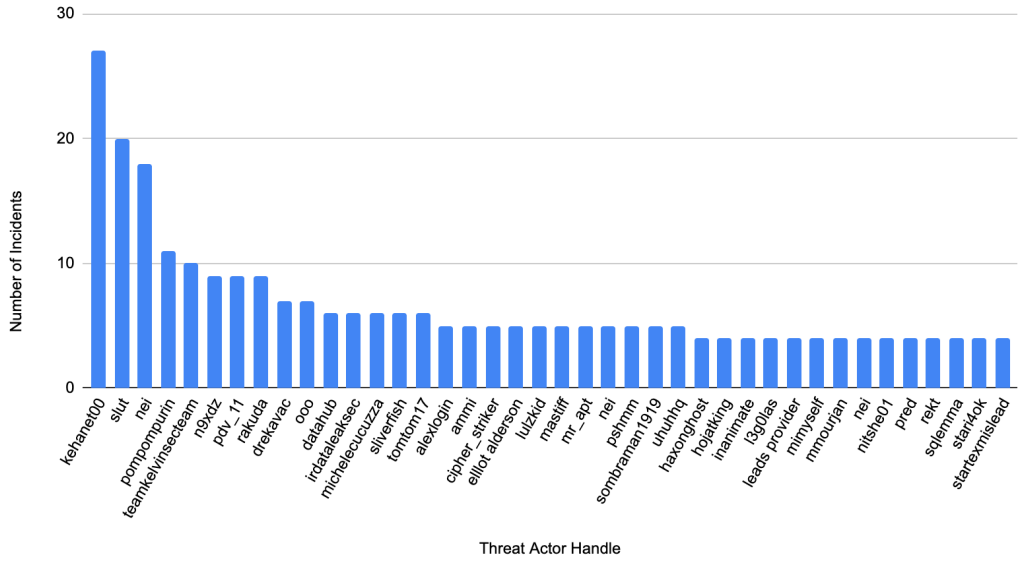
Steps to Preempt Supply Chain Attack Vectors:

- **Protection from client-side attack vectors:**
    - Client applications like web browsers are easy targets for phishing attacks. Hence, user awareness and mandatory cyber hygiene are important.
    - Do not trust unknown emails or emails with suspicious attachments and links.
    - Open attachments in a sandbox.
    - Update your browser applications regularly.

- **Application Security:** Insecure web applications hosting backend databases are a common reason for the occurrence of cyberattacks. Attackers inject code that can manipulate backend systems to compromise data. So, it is important to ensure:
    - Proper input validation to prevent code injections.
    - Use of properly configured WAF (Web Application Firewall).
    - Database management systems and elastic clusters are not connected to the Internet without complex credentials and proper configurations in place.
    - Use of MFA (Multi-factor Authentication) for admin accounts of Internet-facing applications.
    - Periodic web application security audits.
- **Protection of networks -** Endpoint/host security is critical when it comes to network security. A single shot compromise increases the risk of the entire network being taken over by the attacker. Attacks can be prevented by:
    - Installing effective EDRs/XDRs with advanced threat analytics.
    - Proper segmentation and isolation of network based on role and functionality by NGFW (NextGen Firewalls).
    - Deploying IDPS systems strategically to network segments to monitor network anomalies.
    - Setting up a SOC with SIEMS and TI pipeline for proactive threat monitoring.

Prominent Threat Actors

We have identified several major threat actors who have been actively targeting governments and businesses around the globe. These threat actors have posted leaked databases, accesses, vulnerabilities/ exploits, etc., across cybercrime forums. The graph below shows the activity of 40 major threat actors and the number of cyber attacks they have perpetrated. Among these, a threat actor who goes by the handle “Kehanet00” has posted more data leaks and accesses than any other threat actor.



Prominent threat actors

Many of these threat actors are hacktivists, sponsored threat agents, cyber terrorists, script kiddies, organized cybercriminals, etc.

Conclusion

Given the expansion of attack surfaces and the increasing sophistication of threat actors’ tactics, CloudSEK Threat Analysts are continuously analyzing the latest trends and patterns. During Q2 of 2021 we have observed threat actors selling databases, logs, accesses, and exploits that affected organizations across the world. Hence, it is important to monitor cybersecurity trends and the latest developments in adversary tactics, tools, and procedures.

About CloudSEK

CloudSEK is an AI-driven Digital Risk Management Enterprise. CloudSEK's XVigil platform helps clients assess their security posture in real-time from the perspective of an attacker. XVigil scours thousands of sources (across the surface, deep and dark web), to detect cyber threats, data leaks, brand threats, identity thefts, etc. To learn more about how the CloudSEK XVigil platform can strengthen your external security posture and deliver value from Day 1, visit https://cloudsek.com/ or drop a note to sales@cloudsek.com.