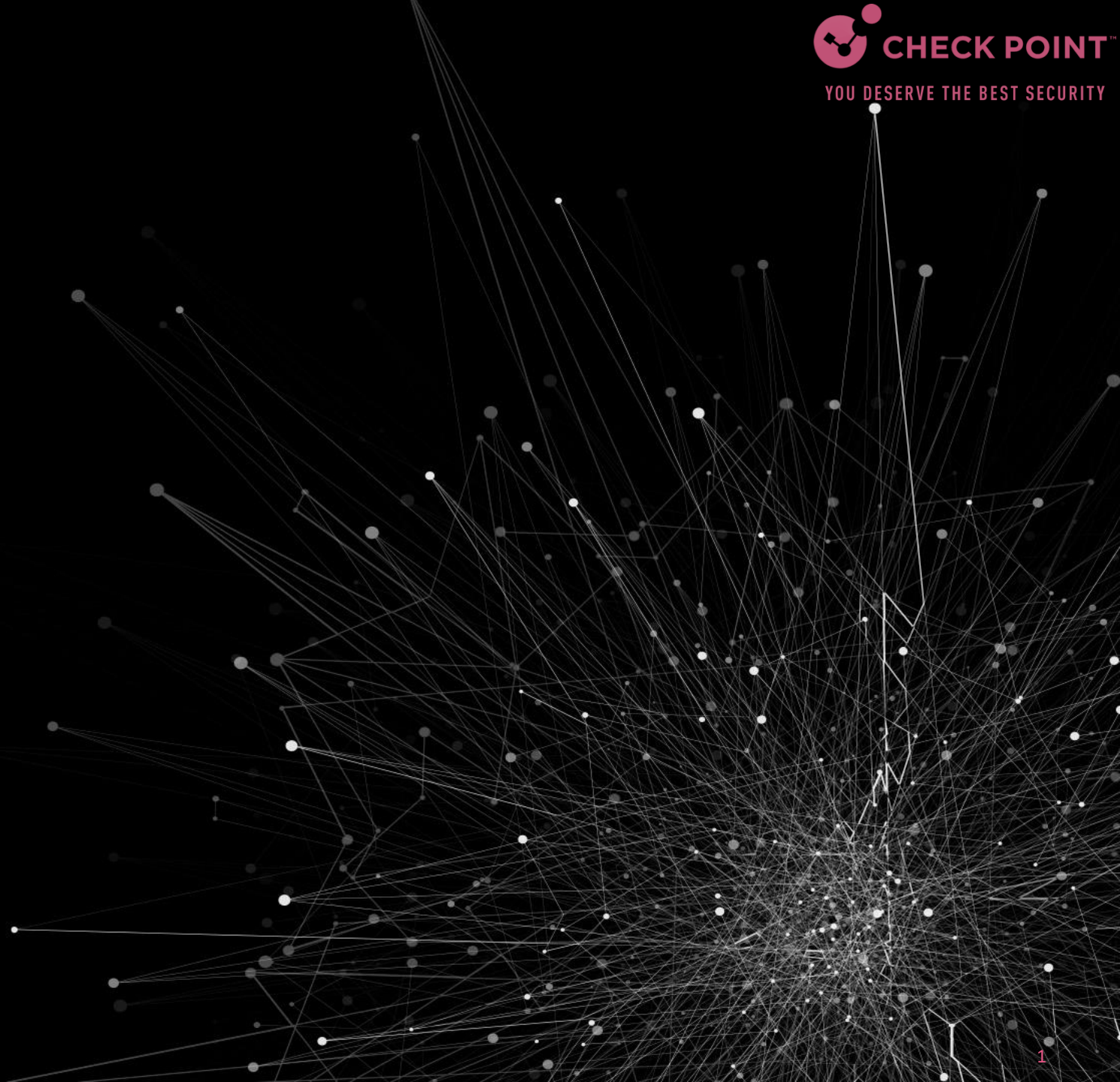
CHECK POINT
YOU DESERVE THE BEST SECURITY

THREAT
INTELLIGENCE
REPORT

Costa Rica



cp<r>
CHECK POINT RESEARCH

Threat Intelligence Summary

- An organization in Costa Rica is being attacked on average 1468 times per week in the last 6 months, compared to 944 attacks per organization in Americas.
- The top malware in Costa Rica is Emotet, impacting 8% of organizations.
- The top malware list in Costa Rica includes 2 Botnets, 1 Backdoor (Tofsee), 1 Banking Trojan (Trickbot) and 1 Infostealer (Formbook).
- 85% of the malicious files in Costa Rica were delivered via Web in the last 30 days.
- The most common vulnerability exploit type in Costa Rica is Remote Code Execution, impacting 73% of the organizations.
- Weekly impacted organizations by malware types:

	Cryptominer	Ransomware	Mobile	InfoStealer	Banking	Botnet
Costa Rica Avg.	8.6%	0.9%	0.1%	3.5%	3.0%	7.3%
Americas Avg.	2.8%	1.2%	1.8%	1.8%	1.4%	4.0%

- View the latest publications by Check Point Research

Threat Landscape

- **Supply chain attacks** - The infamous SolarWinds attack laid the foundations for a supply chain attack frenzy. The past year saw numerous sophisticated attacks such as Codecov in April and Kaseya in July, concluding with the Log4j vulnerability that was exposed in December. The striking impact achieved by this one vulnerability in an open-source library demonstrates the immense inherent risk in software supply chains.
- **Cyber-attacks disrupting everyday life** - The past year saw a large number of attacks targeting critical infrastructure which led to huge disruption to individuals' day-to-day lives, and in some cases even threatened their sense of physical security.
- **Cloud services under attack** - Cloud provider vulnerabilities became much more alarming in the past year than they were previously. The vulnerabilities exposed throughout the year have allowed attackers, for varying timeframes, to execute arbitrary code, escalate to root privileges, access mass amounts of private content, and even cross between different environments.
- **Developments in the mobile landscape** - Throughout the year, threat actors have increasingly used smishing (SMS phishing) for malware distribution and have invested substantial efforts in hacking social media accounts to obtain access to mobile devices. The continued digitization of the banking sector in the past year led to the introduction of various apps designed to limit face-to-face interactions, and those, in turn, have led to the distribution of new threats.
- **Cracks in the ransomware ecosystem** - Governments and law enforcement agencies changed their stance on organized ransomware groups in the past year, turning from preemptive and reactive measures to proactive offensive operations against the ransomware operators, their funds, and supporting infrastructure. The major shift happened following the Colonial Pipeline incident in May which made the Biden administration realize they had to step up efforts to combat this threat.
- For more data and examples please see Check Point Research Cyber Attack Trends: 2022 Annual Report.

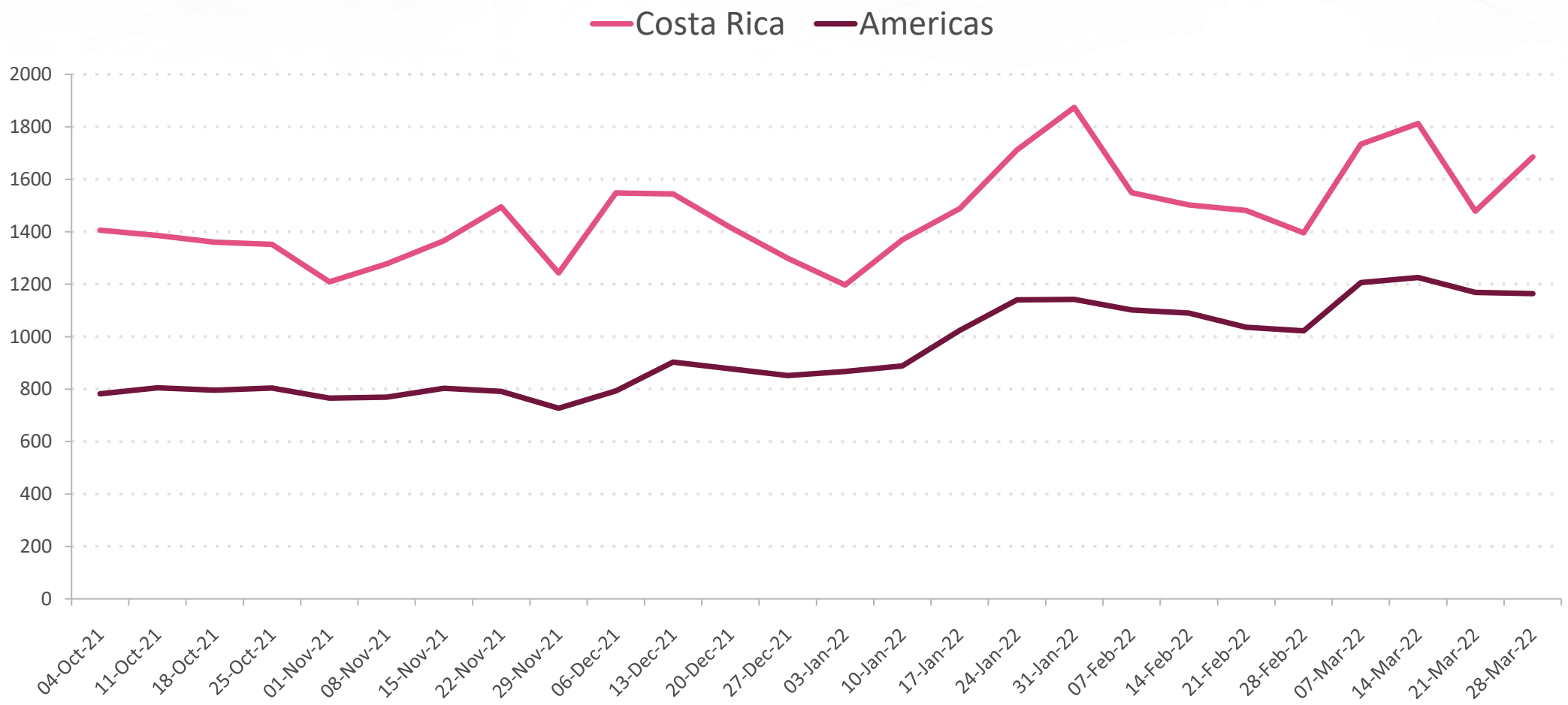
Major attacks and data breaches - Costa Rica

- Jun-20 - Following its reported attack earlier this year on the state-owned Bank of Costa Rica, the Maze group, infamous for a recent wave of double-extortion attacks, has started releasing payment card data obtained in the attack. The group reports it is in possession of some 4 million unique payment card numbers, including 140,000 allegedly belonging to U.S. customers.
  - Check Point SandBlast and Anti-Bot provide protection against this threat(Ransomware.Win32.Maze)
- May-20 - Maze ransomware operators claim to have stolen 11 million credit card credentials from the state-owned Bank of Costa Rica Banco BCR. The Maze group, infamous for its recent double-extortion routine, explained it did not encrypt the banks documents due to the world pandemic.
  - Check Point SandBlast and Anti-Bot provide protection against this threat (Ransomware.Win32.Maze)

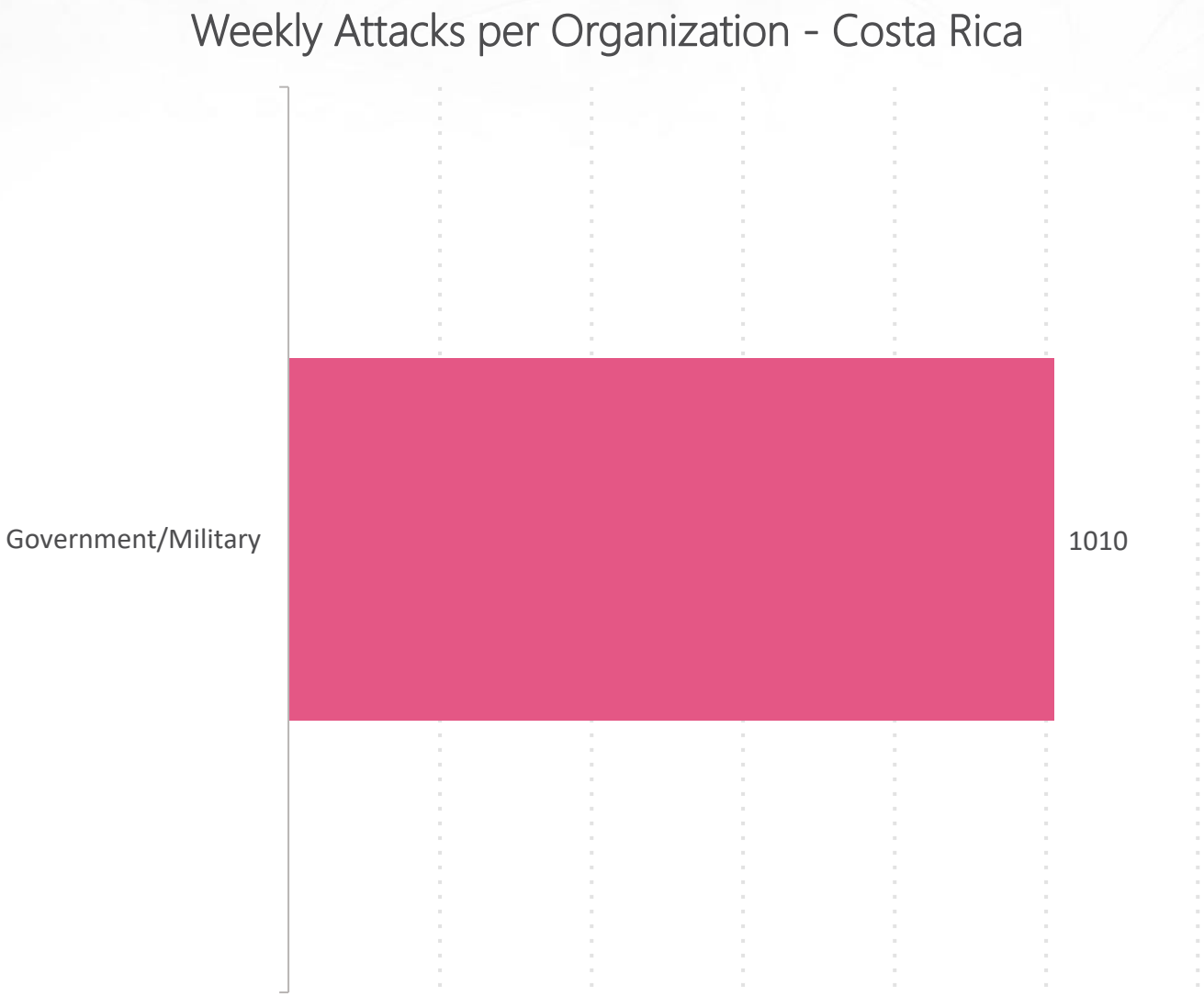
Major attacks and data breaches - Americas

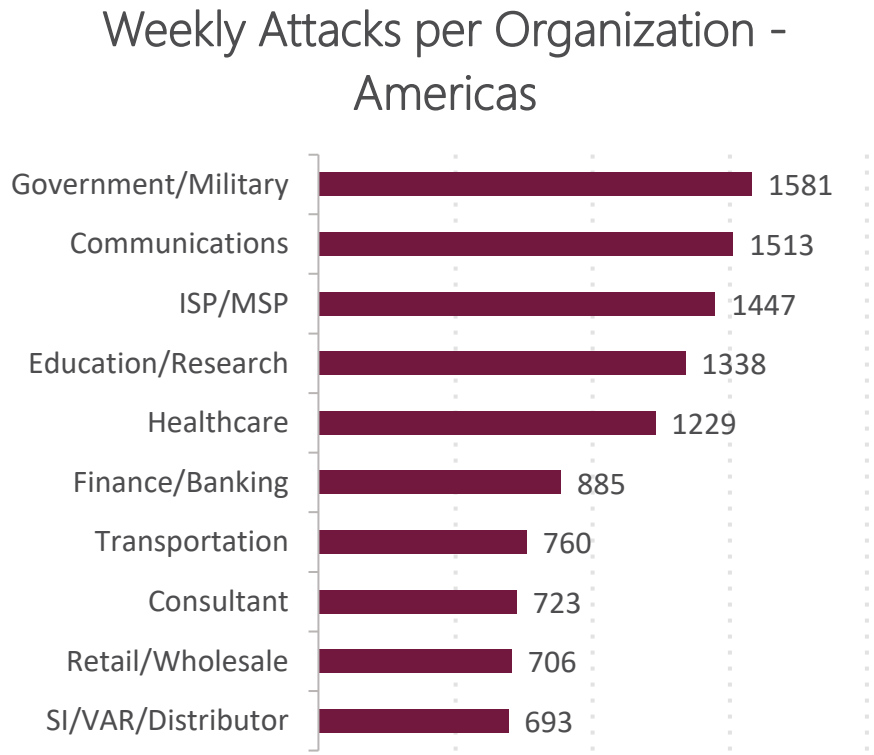
- Mar-22 - The FBI warns of US critical infrastructure sectors, including financial services, critical manufacturing, government facilities and more, being targeted with the AvosLocker ransomware.
- Mar-22 - TransUnion South Africa has been victim of a breach in which the hacker group named N4aughtysecTU stole 4TB of data. Attackers who claim to be based in Brazil are demanding a $15 million ransom over the sensitive data which includes credit score, banking details and ID numbers.
- Mar-22 - State-sponsored APT41 group (aka Wicked Panda) affiliated with China has been successfully breaching into US government networks for the past 6 months by exploiting vulnerable web facing applications. Vulnerabilities included Log4Shell and a zero-day flaw in the USAHerds app tracked CVE-2021-44207.
- Mar-22 - US insurance broker AON is investigating a cyber-attack that has impacted part of their systems.
- Feb-22 - Check Point Research has spotted a new malware, Electron-bot, distributed through gaming applications on Microsoft's official store, with at least 5,000 victims, mostly in Sweden, Bulgaria, Russia, Bermuda and Spain. The malware can control social media accounts of its victims, including Facebook, Google and Sound Cloud. The malware can register new accounts, log in, comment on and like other posts.
- Feb-22 - Researchers have published details of Bvp47, a backdoor used by the Equation APT group, allegedly linked to the US National Security Agency (NSA). Bvp47 has been used on over 287 targets located in 45 countries, mainly China, Korea, Japan, Germany, Spain, India and Mexico.

Attacks per Organization - Last 6 Months



Most Impacted Industries - Last 6 Months





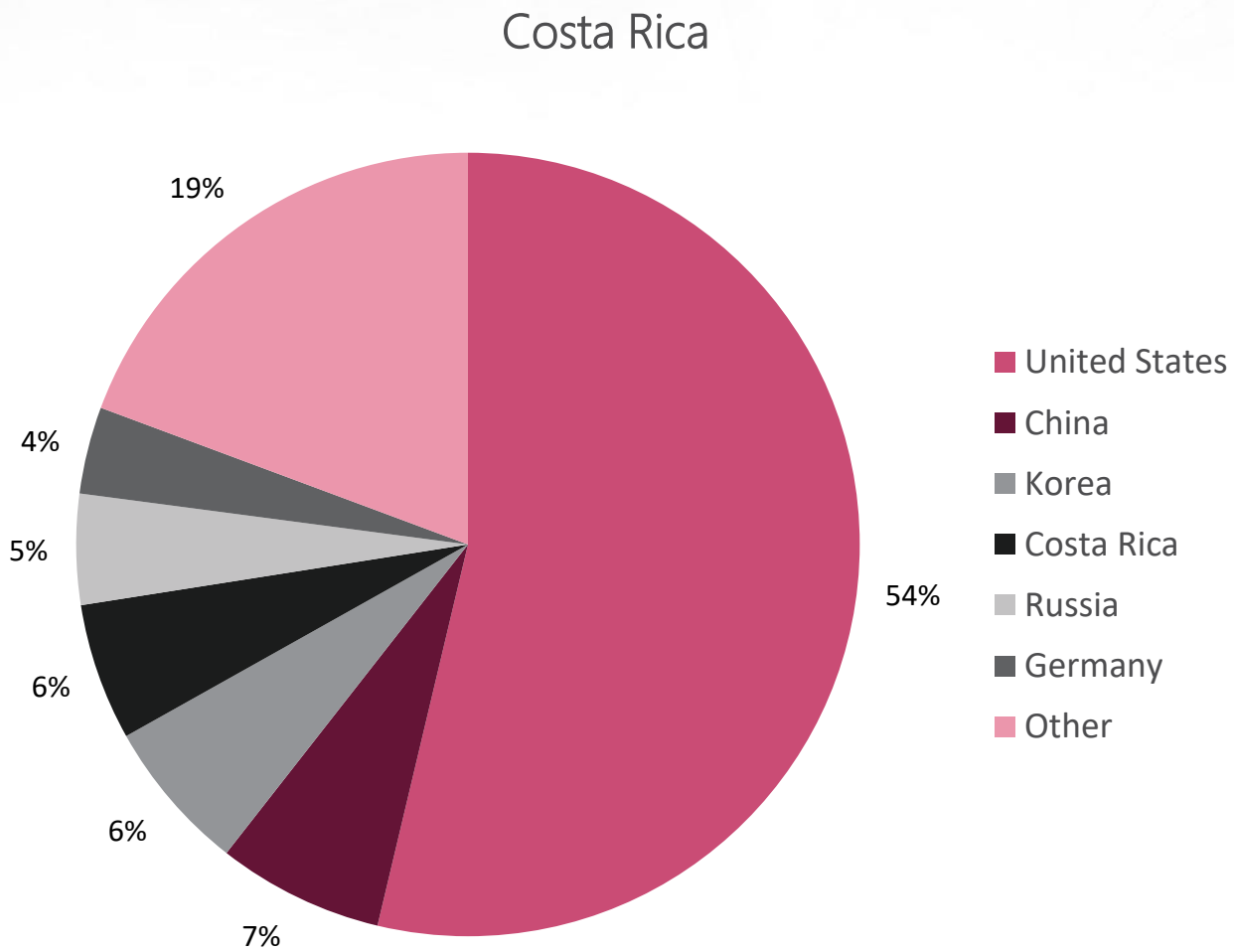
Top Malware - Costa Rica- Feb-22

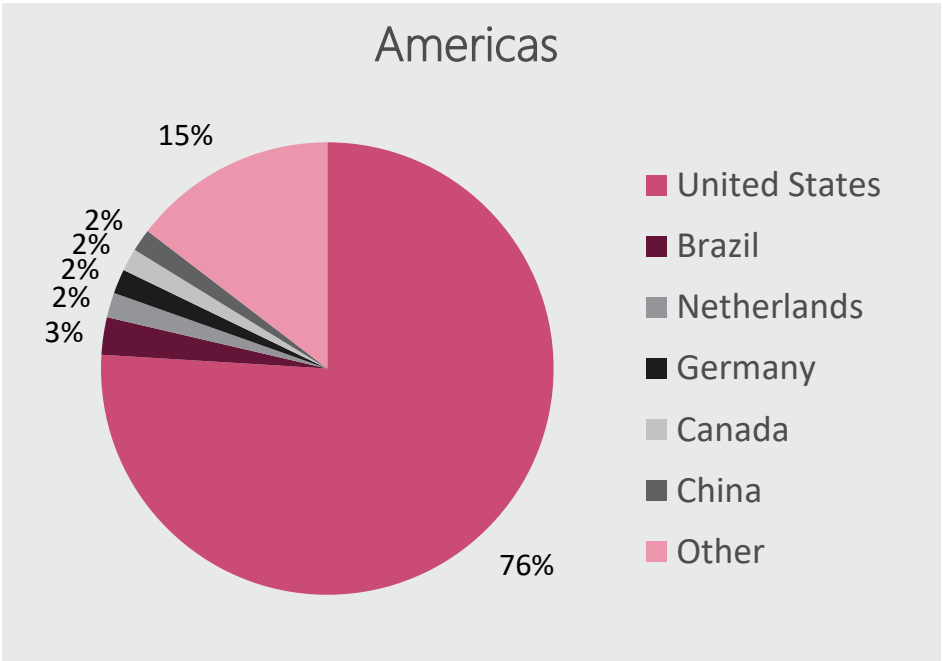
MALWARE FAMILY	COSTA RICA IMPACT	AMERICAS IMPACT	DESCRIPTION
Emotet	8%	4%	Emotet is an advanced, self-propagating and modular Trojan that was once used as a banking Trojan, and currently distributes other malware or malicious campaigns. Emotet uses multiple methods for maintaining persistence and evasion techniques to avoid detection and can be spread via phishing spam emails containing malicious attachments or links.
Formbook	3%	2%	FormBook is an Infostealer targeting the Windows OS and was first detected in 2016. It is marketed as Malware as a Service (MaaS) in underground hacking forums for its strong evasion techniques and relatively low price. FormBook harvests credentials from various web browsers, collects screenshots, monitors and logs keystrokes, and can download and execute files according to orders from its C&C.
Glupteba	3%	1%	Known since 2011, Glupteba is a backdoor that gradually matured into a botnet. By 2019 it included a C&C address update mechanism through public BitCoin lists, an integral browser stealer capability and a router exploiter.
Tofsee	3%	1%	Tofsee is a Trickler that targets the Windows platform. This malware attempts to download and execute additional malicious files on target systems. It may download and display an image file to a user in an effort to hide its true purpose.
Trickbot	3%	1%	Trickbot is a modular banking Trojan, attributed to the WizardSpider cybercrime gang. Mostly delivered via spam campaigns or other malware families such as Emotet and BazarLoader. Trickbot sends information about the infected system and can also download and execute arbitrary modules from a large array of available modules, including a VNC module for remote control and an SMB module for spreading within a compromised network. Once a machine is infected, the threat actors behind this malware, utilize this wide array of modules not only to steal banking credentials from the target PC, but also for lateral movement and reconnaissance on the targeted organization itself, prior to delivering a company-wide targeted ransomware attack.

Top Malware - Americas- Feb-22

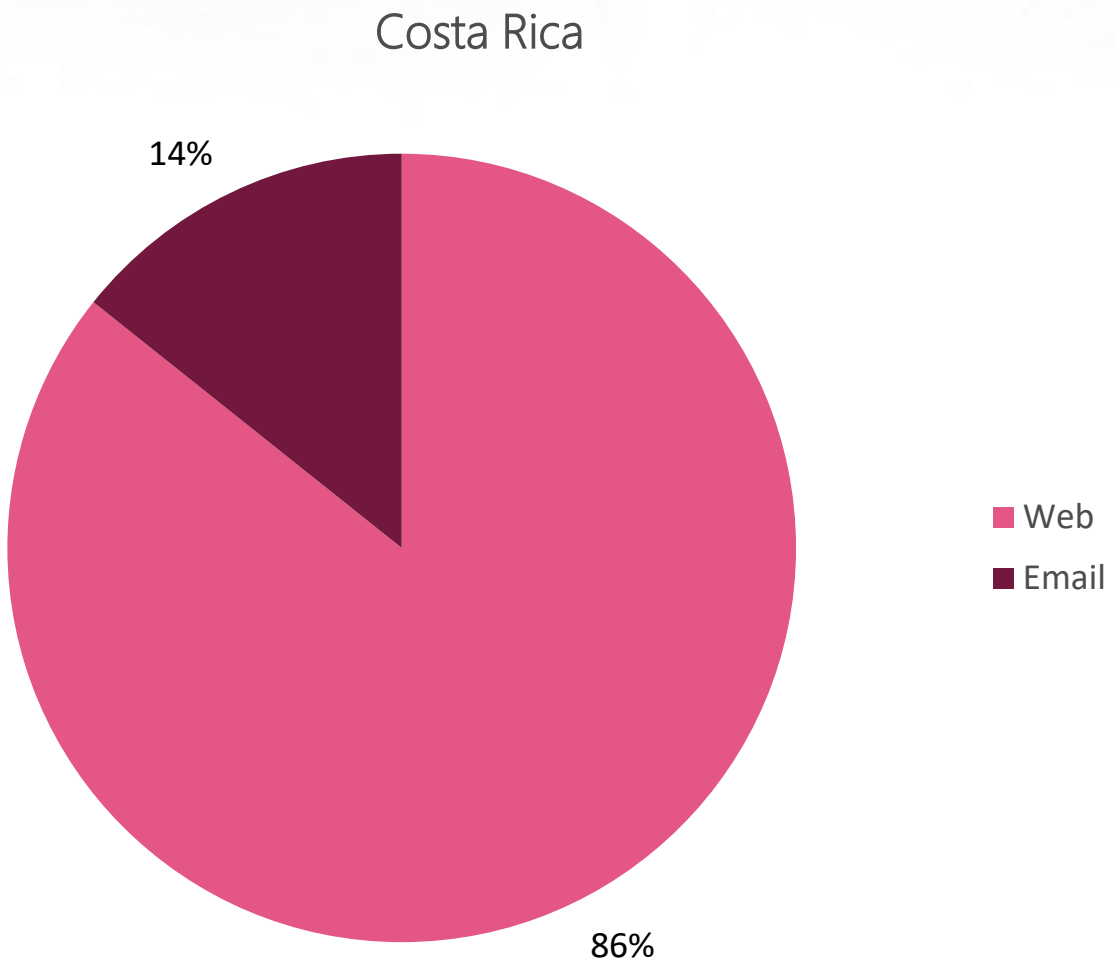
MALWARE FAMILY	AMERICAS IMPACT	DESCRIPTION
Emotet	4%	Emotet is an advanced, self-propagating and modular Trojan that was once used as a banking Trojan, and currently distributes other malware or malicious campaigns. Emotet uses multiple methods for maintaining persistence and evasion techniques to avoid detection and can be spread via phishing spam emails containing malicious attachments or links.
Formbook	2%	FormBook is an Infostealer targeting the Windows OS and was first detected in 2016. It is marketed as Malware as a Service (MaaS) in underground hacking forums for its strong evasion techniques and relatively low price. FormBook harvests credentials from various web browsers, collects screenshots, monitors and logs keystrokes, and can download and execute files according to orders from its C&C.
Trickbot	1%	Trickbot is a modular banking Trojan, attributed to the WizardSpider cybercrime gang. Mostly delivered via spam campaigns or other malware families such as Emotet and BazarLoader. Trickbot sends information about the infected system and can also download and execute arbitrary modules from a large array of available modules, including a VNC module for remote control and an SMB module for spreading within a compromised network. Once a machine is infected, the threat actors behind this malware, utilize this wide array of modules not only to steal banking credentials from the target PC, but also for lateral movement and reconnaissance on the targeted organization itself, prior to delivering a company-wide targeted ransomware attack.
XMRig	1%	XMRig is open-source CPU mining software used to mine the Monero cryptocurrency. Threat actors often abuse this open-source software by integrating it into their malware to conduct illegal mining on victims devices.
Wacatac	1%	Wactac is a Trojan threat that locks files but doesn't encrypt files like typical Ransomware. When Wactac infiltrates the user's system it changes the names of target files by adding a ""wctw"" extension. The lack of ability to encrypt data makes this threat reversible. Usually, Wactac is proliferated by spam email campaigns and fake software.

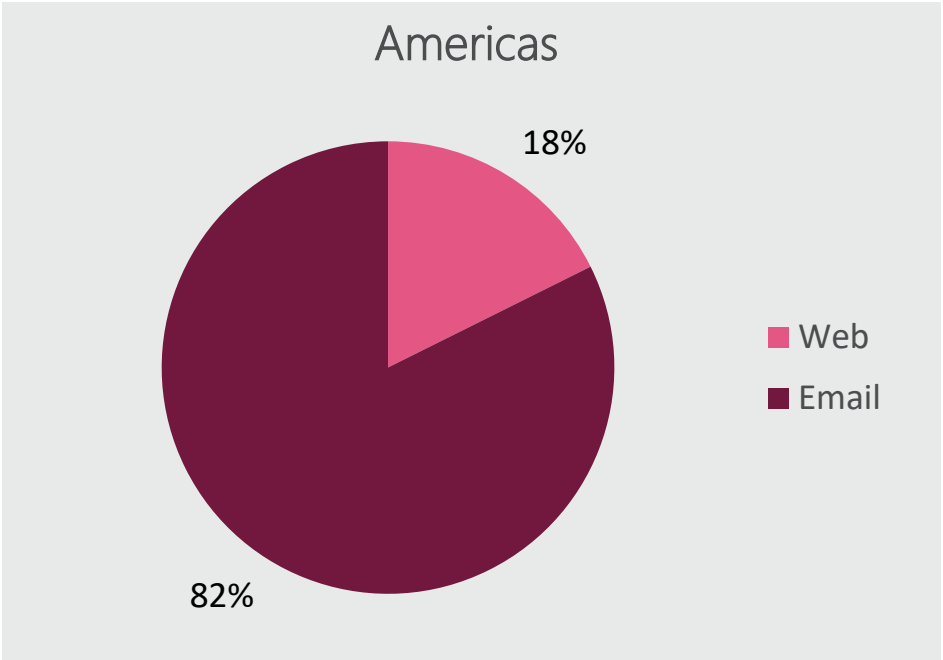
Top Threat Source Countries- Last 6 Months





Attack Vectors for Malicious Files- Last 30 Days

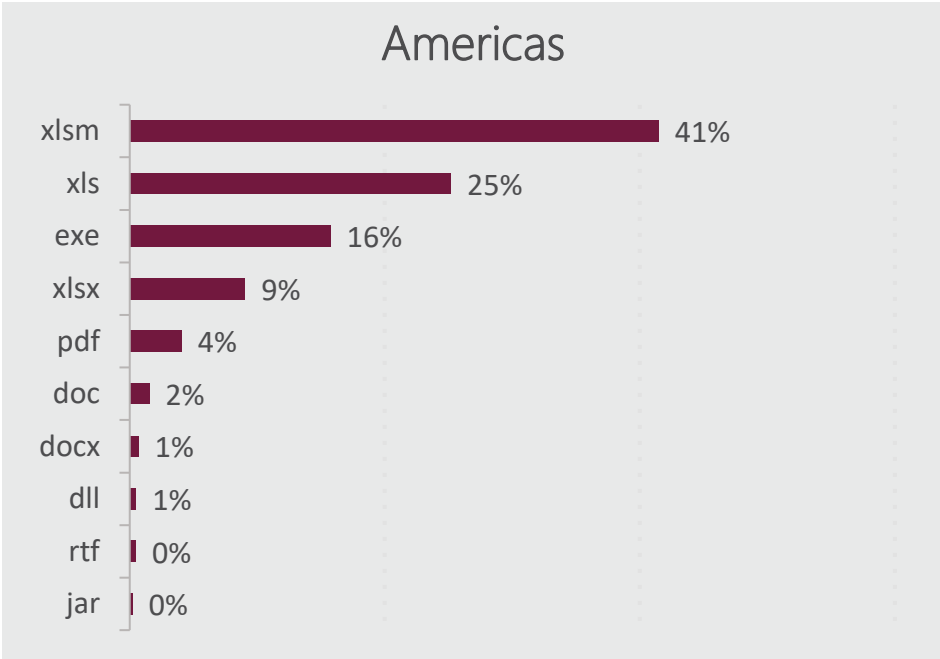




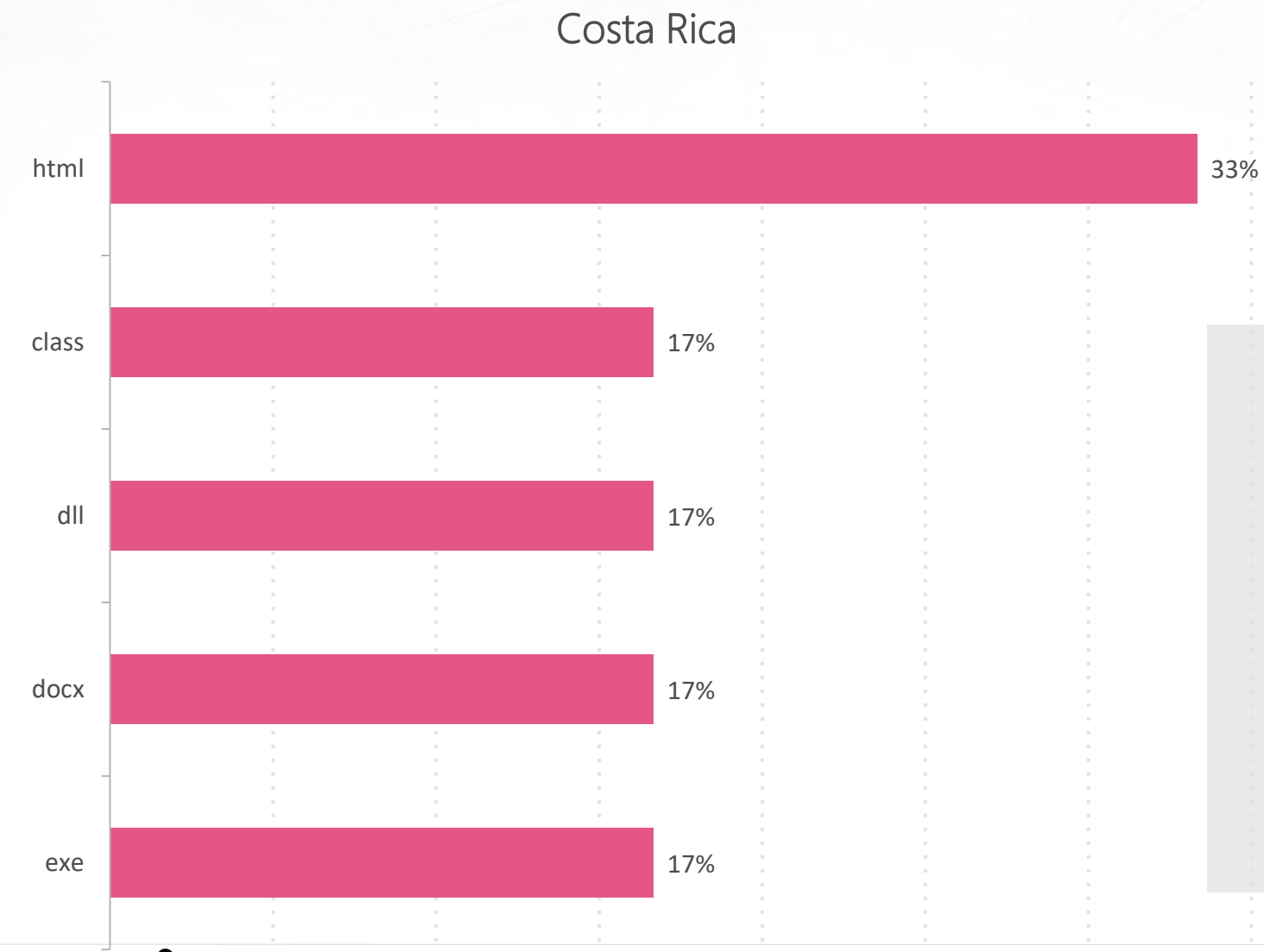
Top Malicious File Types, Email- Last 30 Days

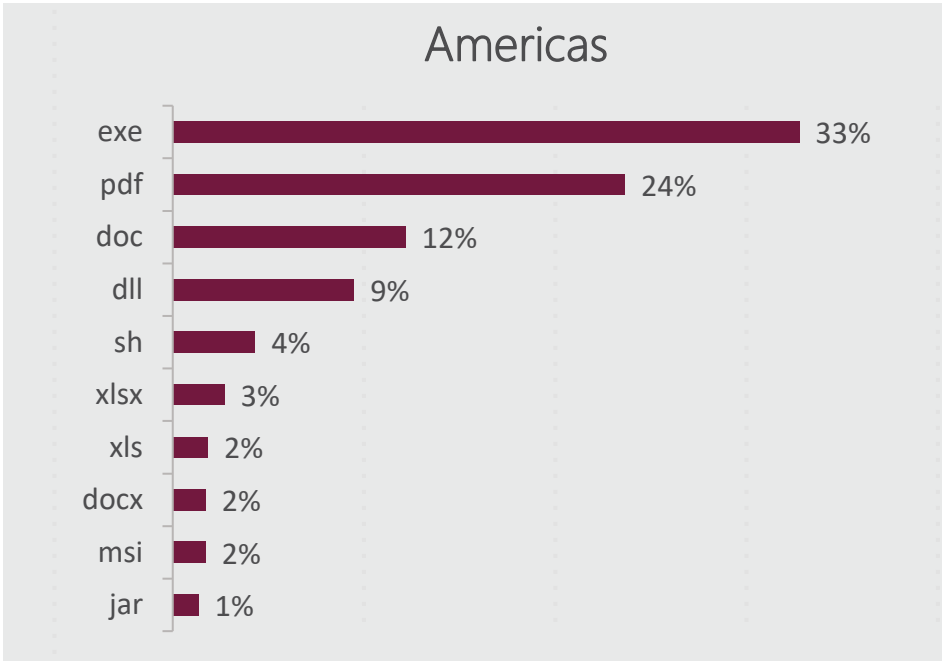
There is insufficient data.

Contact data_research@checkpoint.com for assistance.



Top Malicious File Types, Web- Last 30 Days

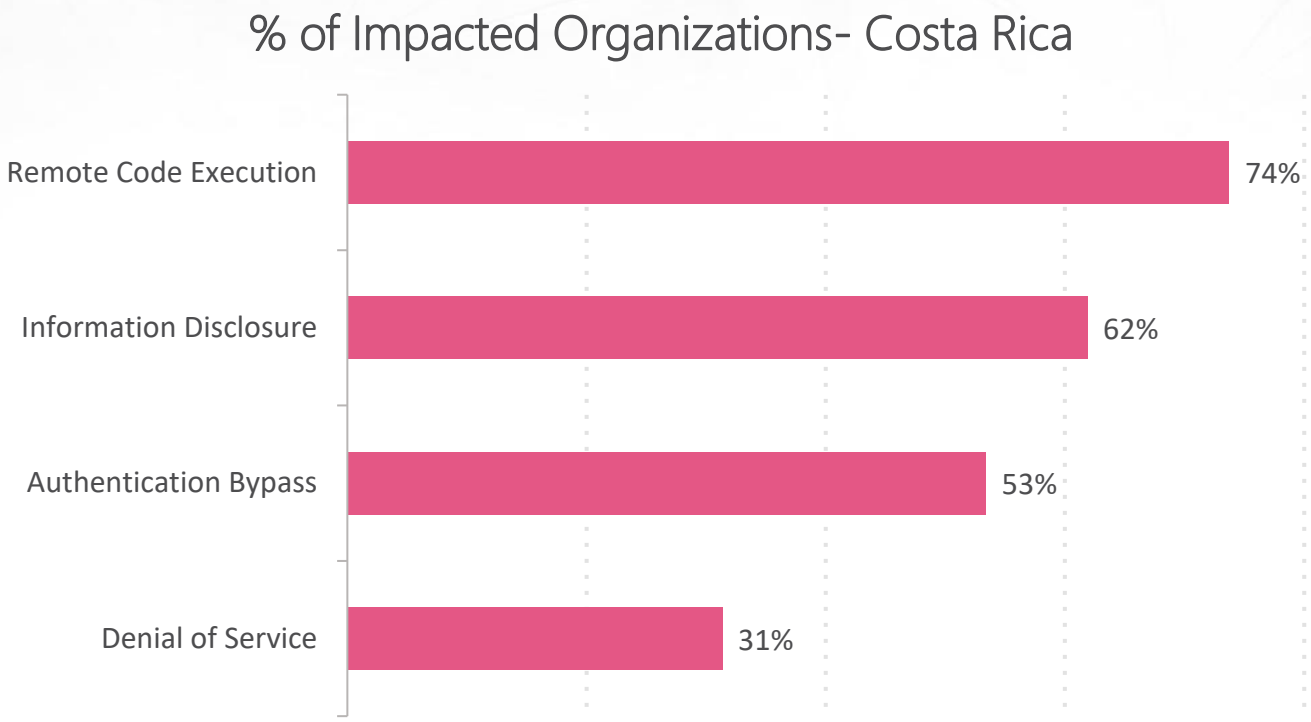


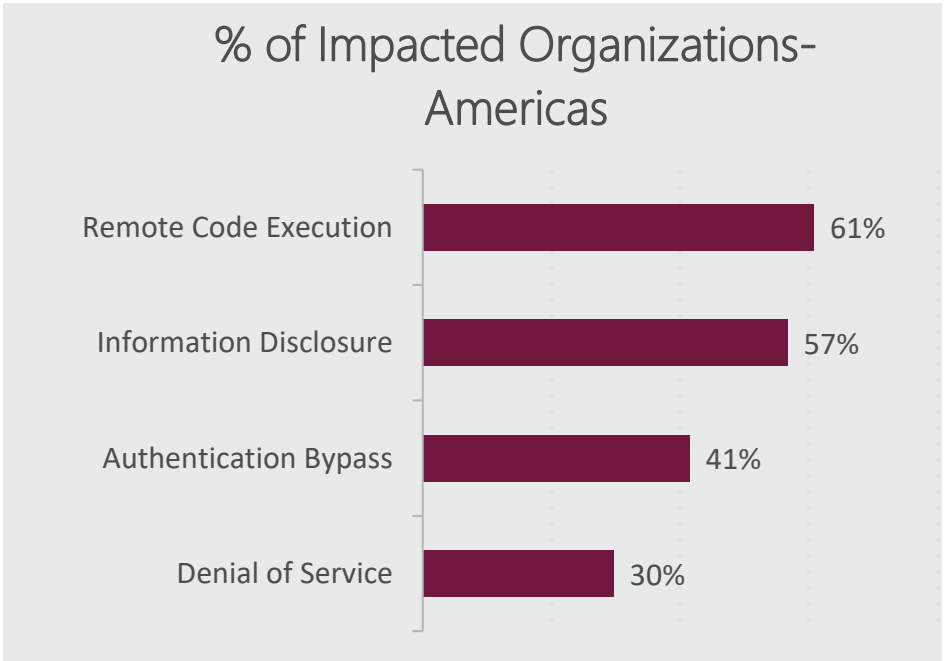


Top MITRE Techniques, Malicious EXE Files- Last 30 Days

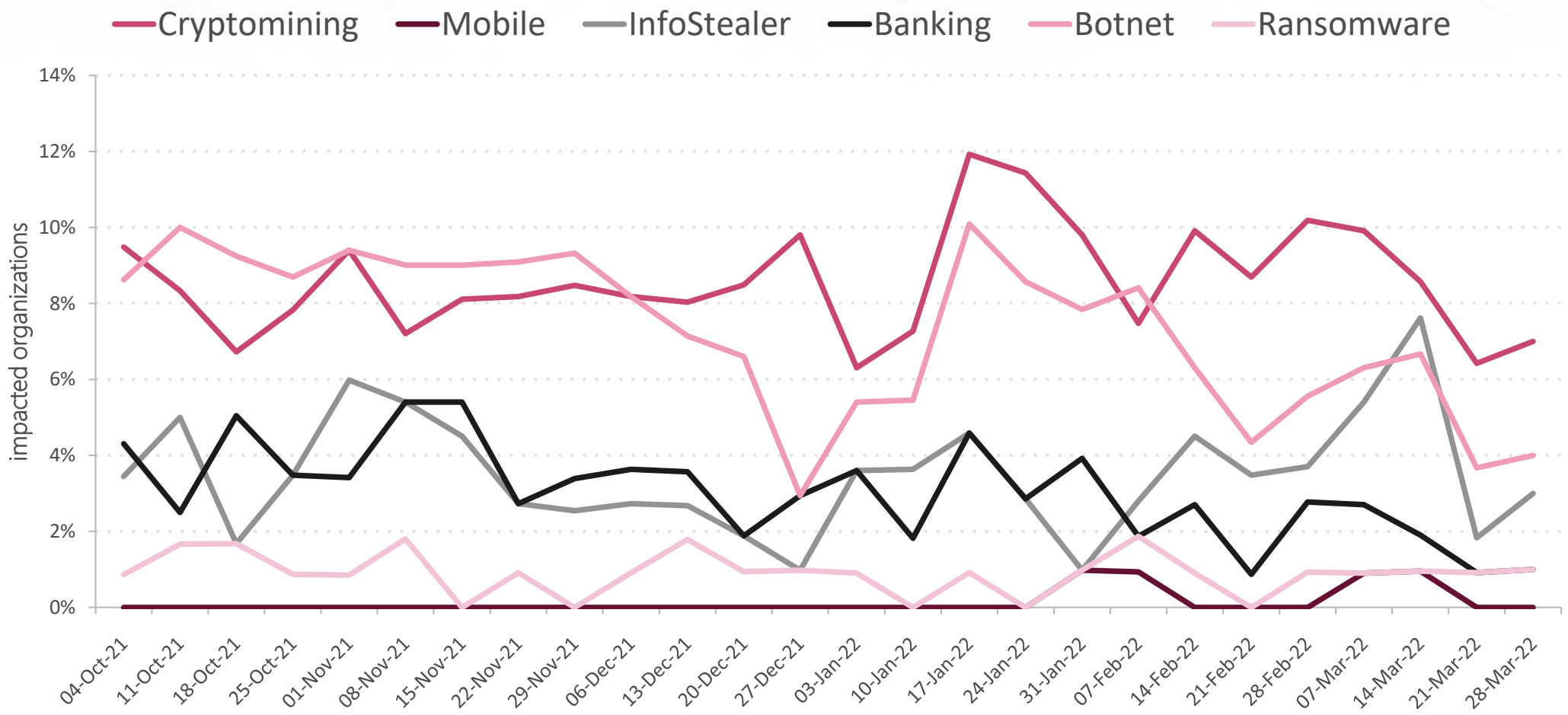
TECHNIQUE	RELATED TACTICS	COSTA RICA IMPACT	AMERICAS IMPACT
Execution through API	Execution	35%	52%
Virtualization / Sandbox Evasion	Defense Evasion, Discovery	28%	44%
Input Capture	Credential Access, Collection	21%	27%
System Information Discovery	Discovery	21%	43%
Hooking	Persistence, Privilege Escalation, Credential Access	21%	25%

Top Vulnerability Exploit types - Last 30 Days

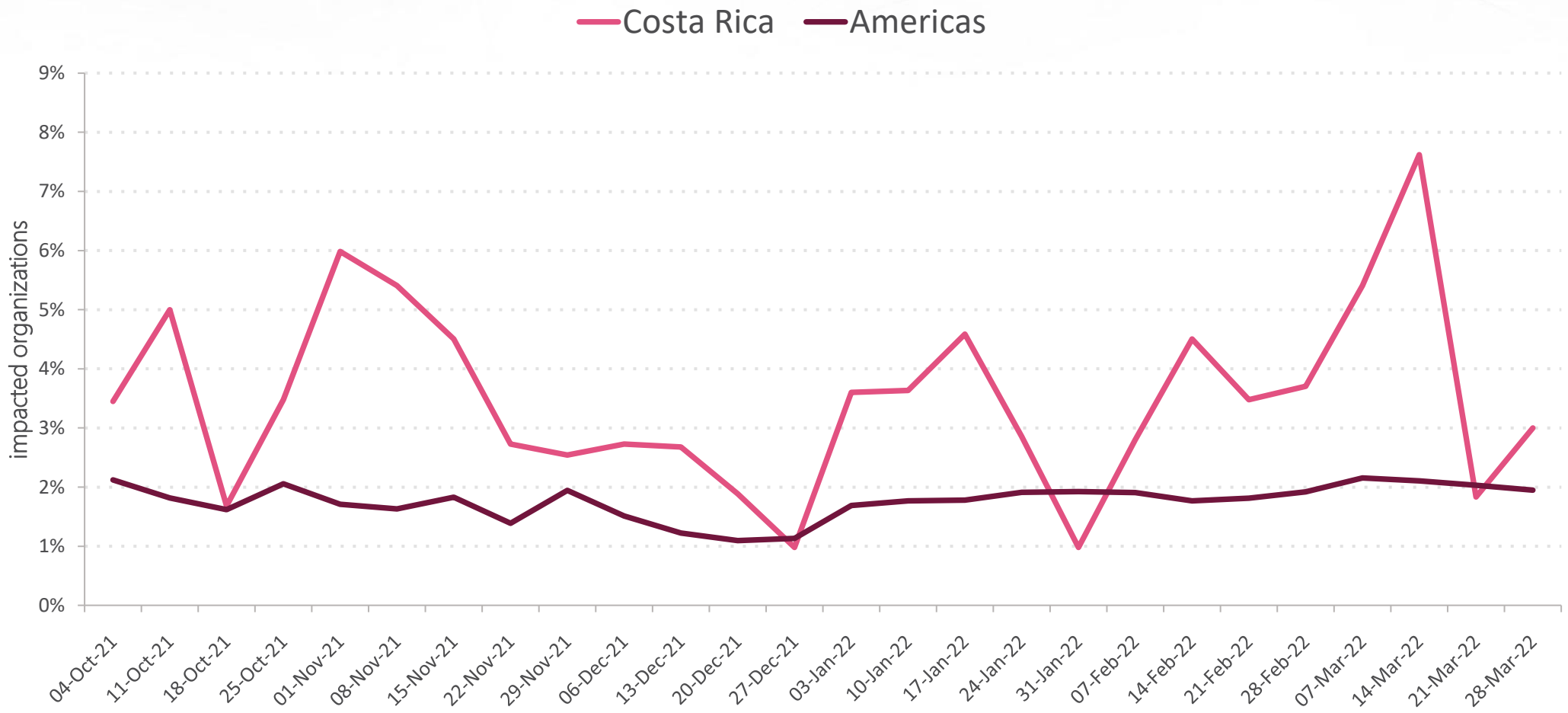




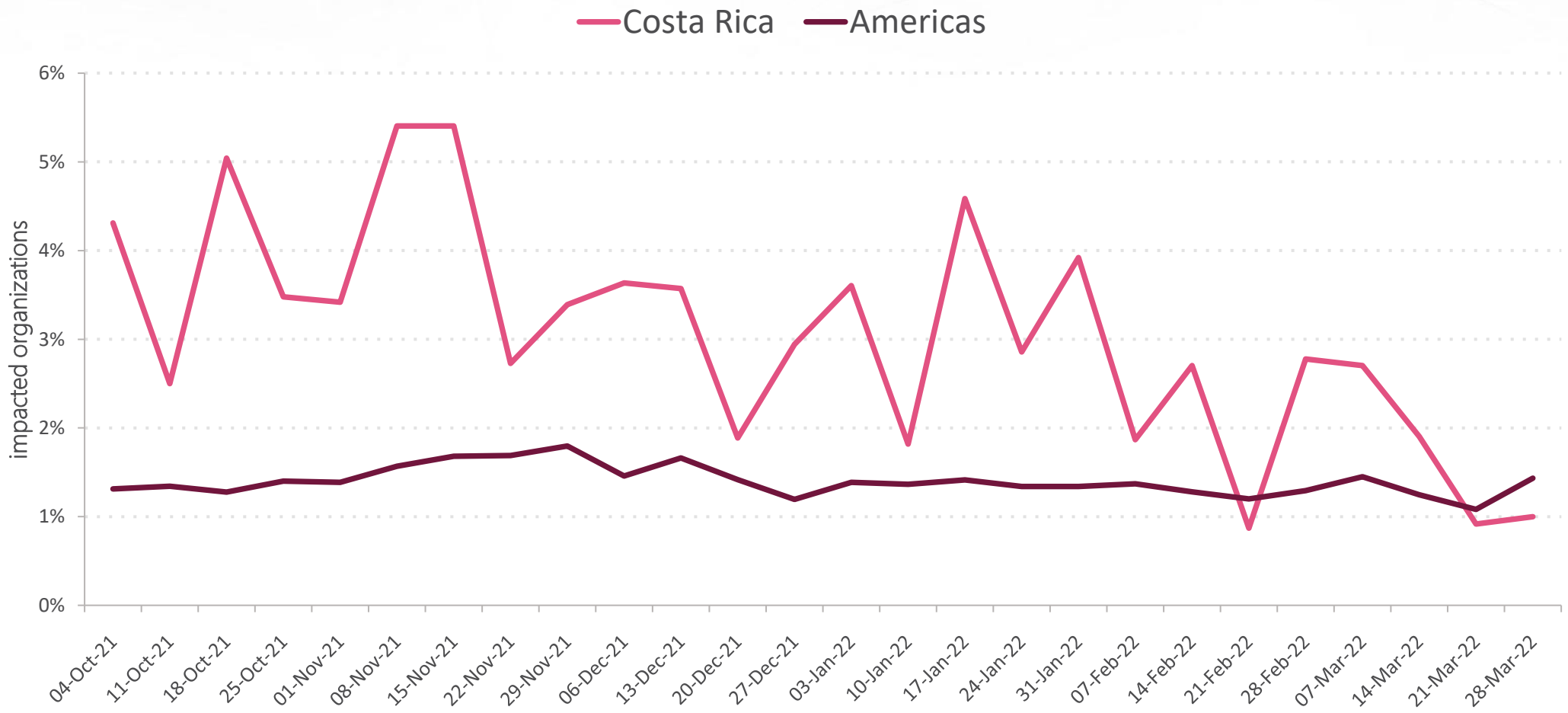
Major Malware Types trend - Costa Rica, Last 6 Months



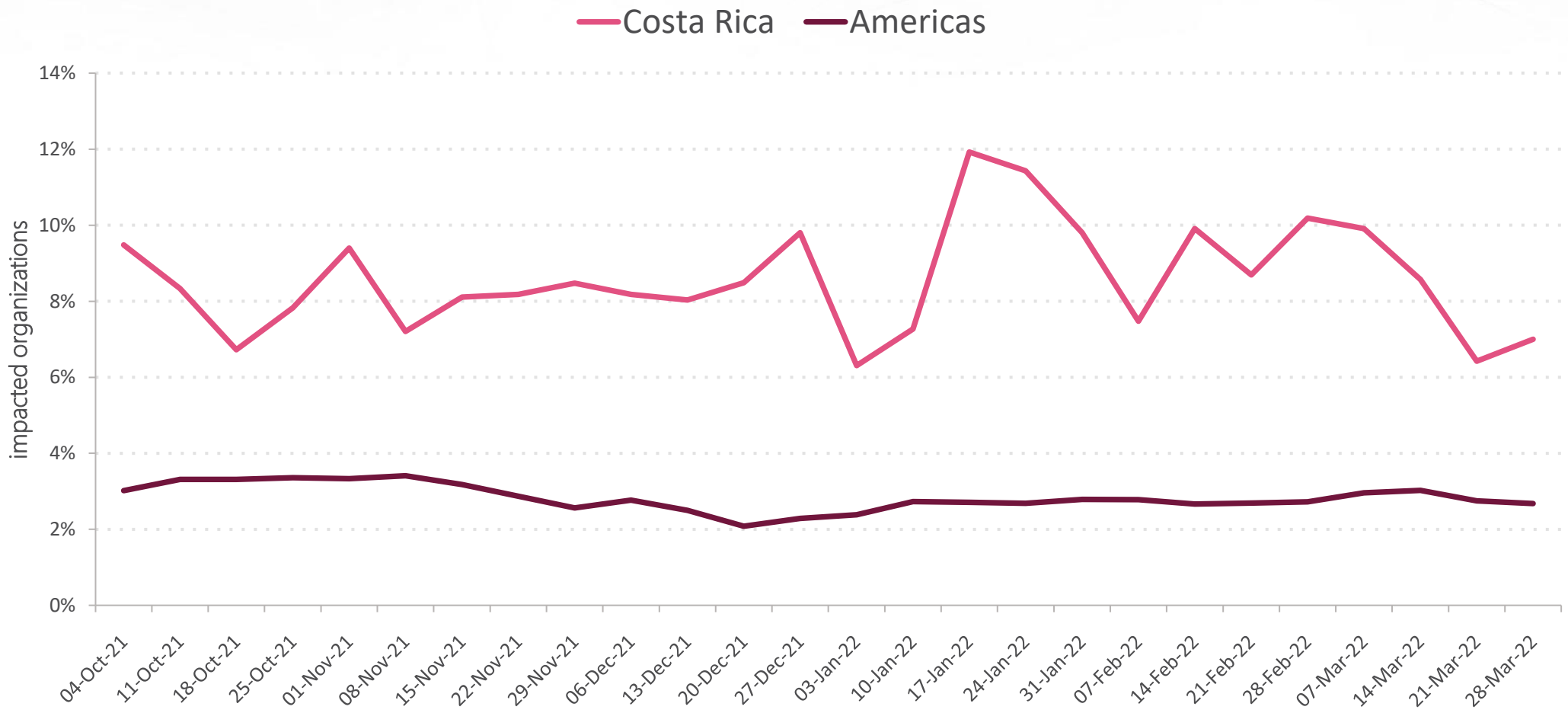
InfoStealer Attacks- Last 6 Months



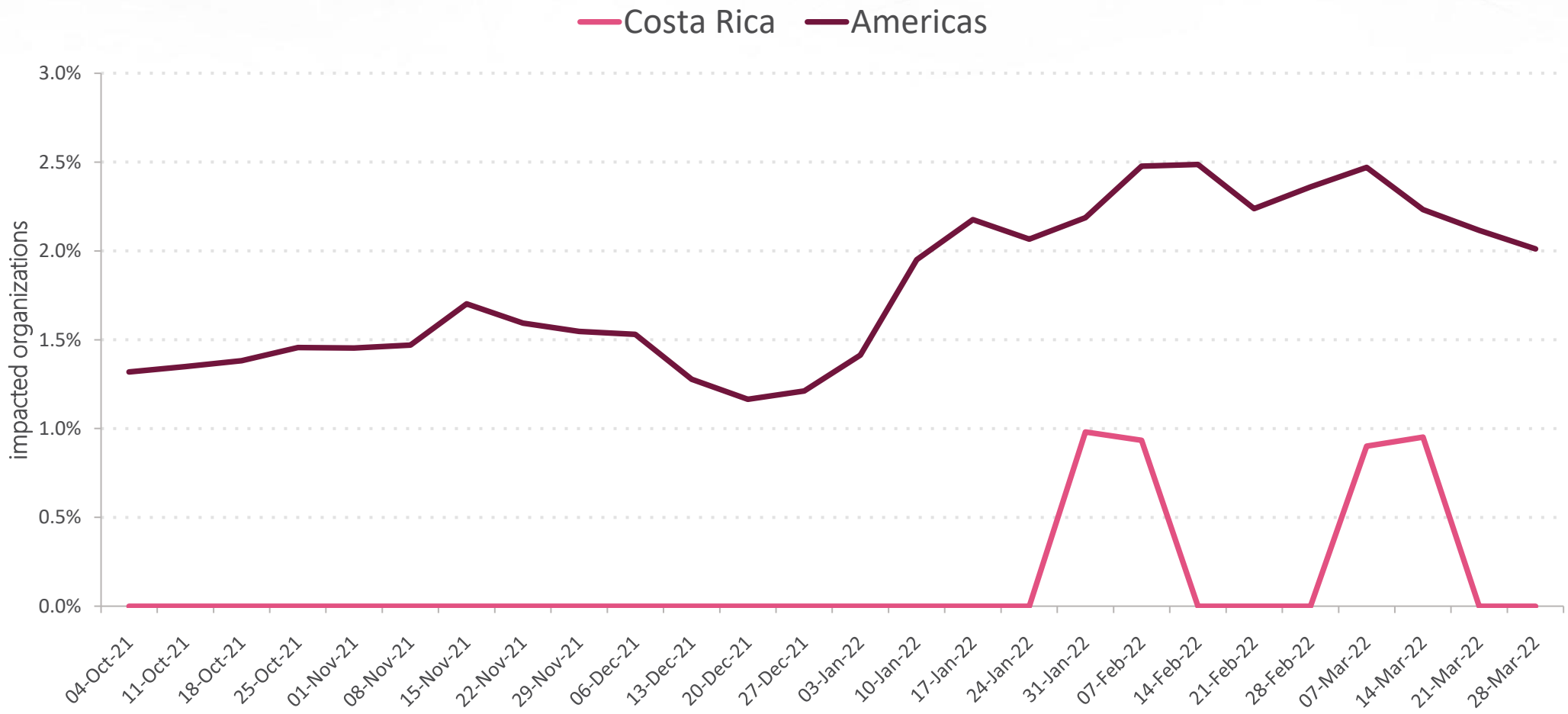
Banking Attacks- Last 6 Months



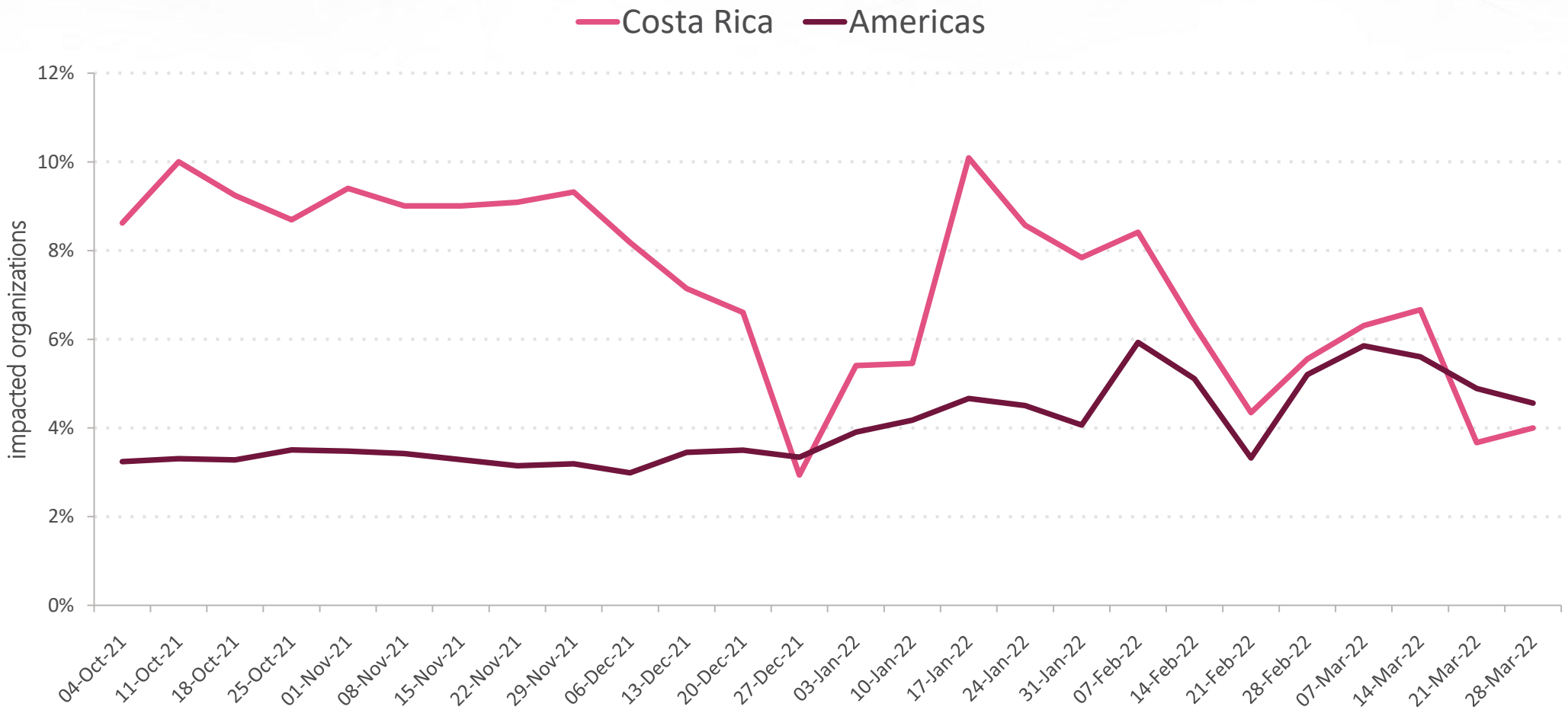
Cryptominer Attacks- Last 6 Months



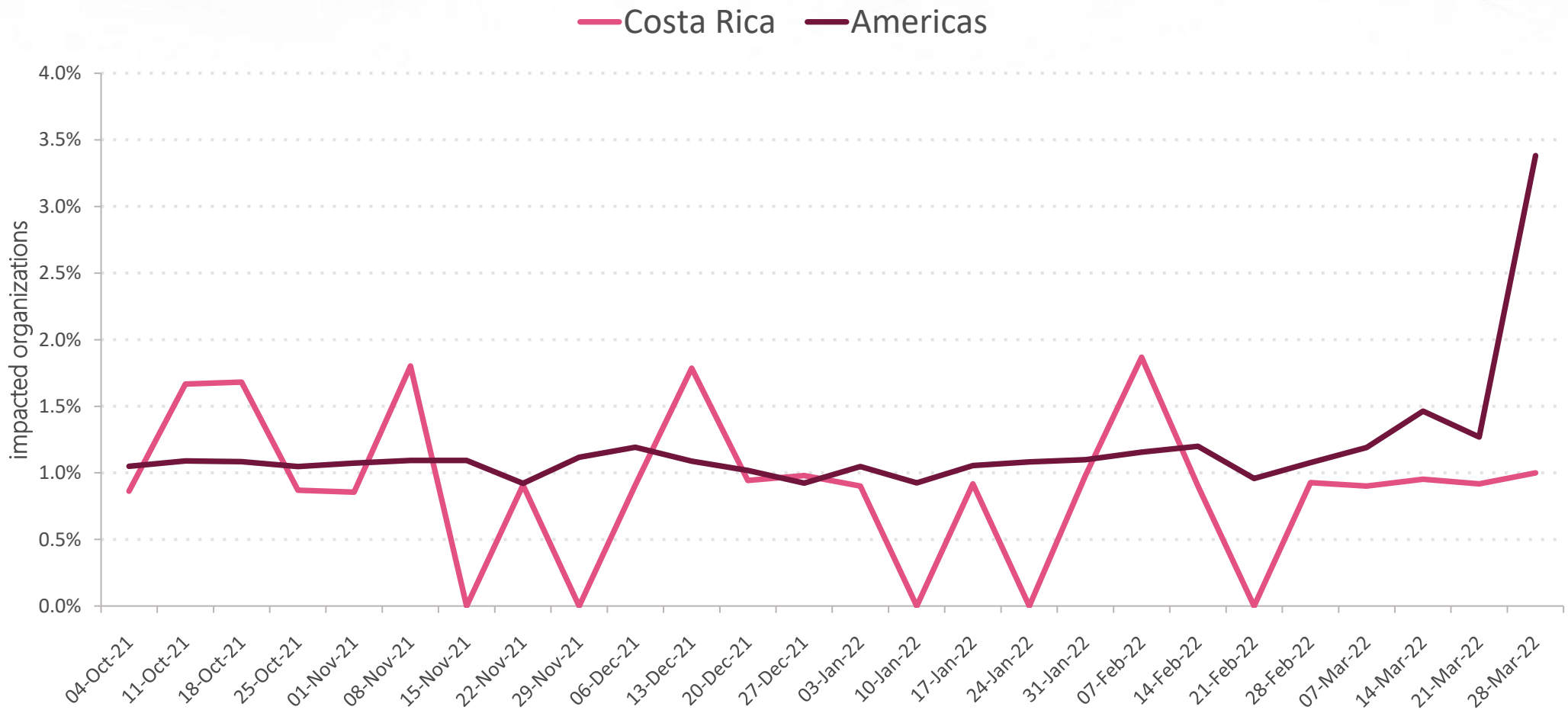
Mobile Attacks- Last 6 Months



Botnet Attacks- Last 6 Months



Ransomware Attacks- Last 6 Months



CHECK POINT
YOU DESERVE THE BEST SECURITY

THREAT
INTELLIGENCE
REPORT

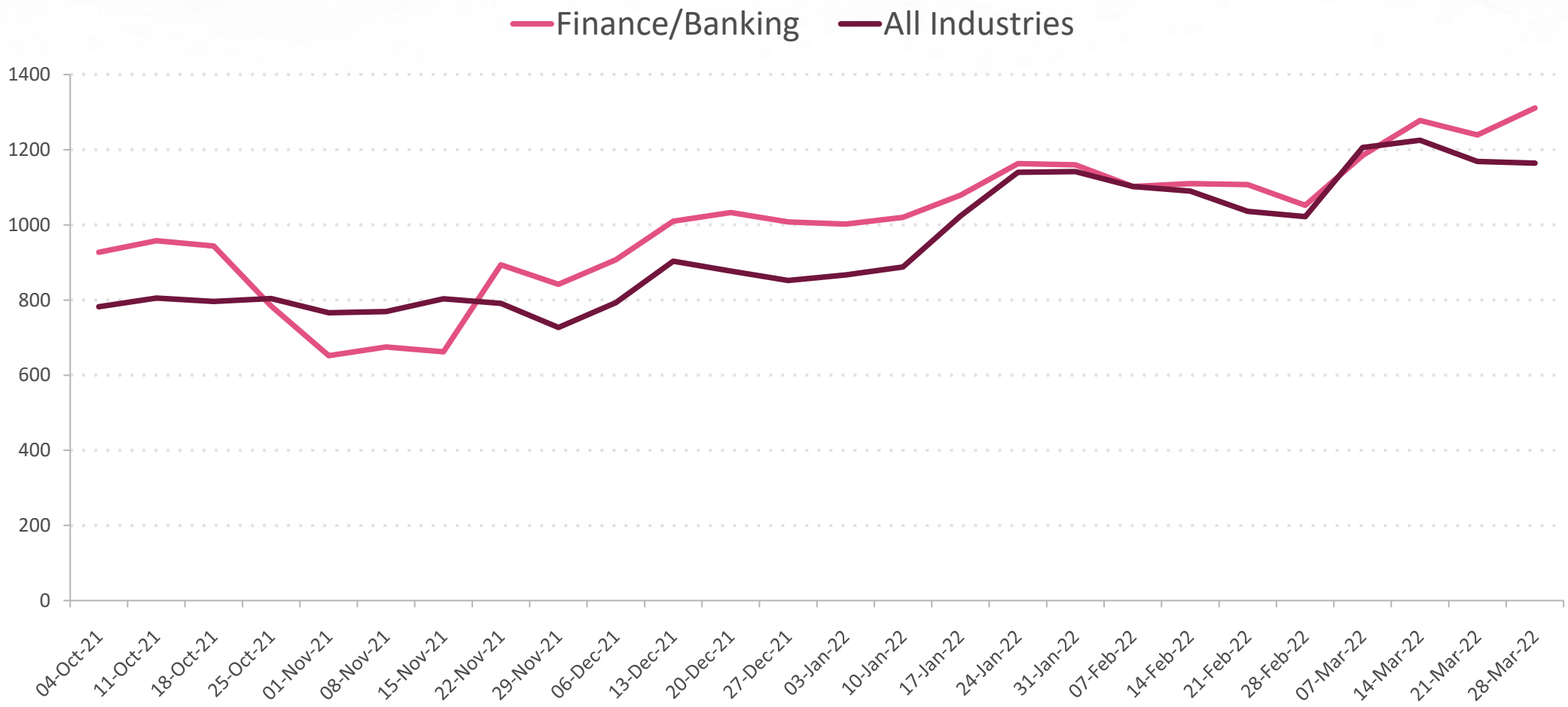
Finance/Banking Americas

cp<r>
CHECK POINT RESEARCH

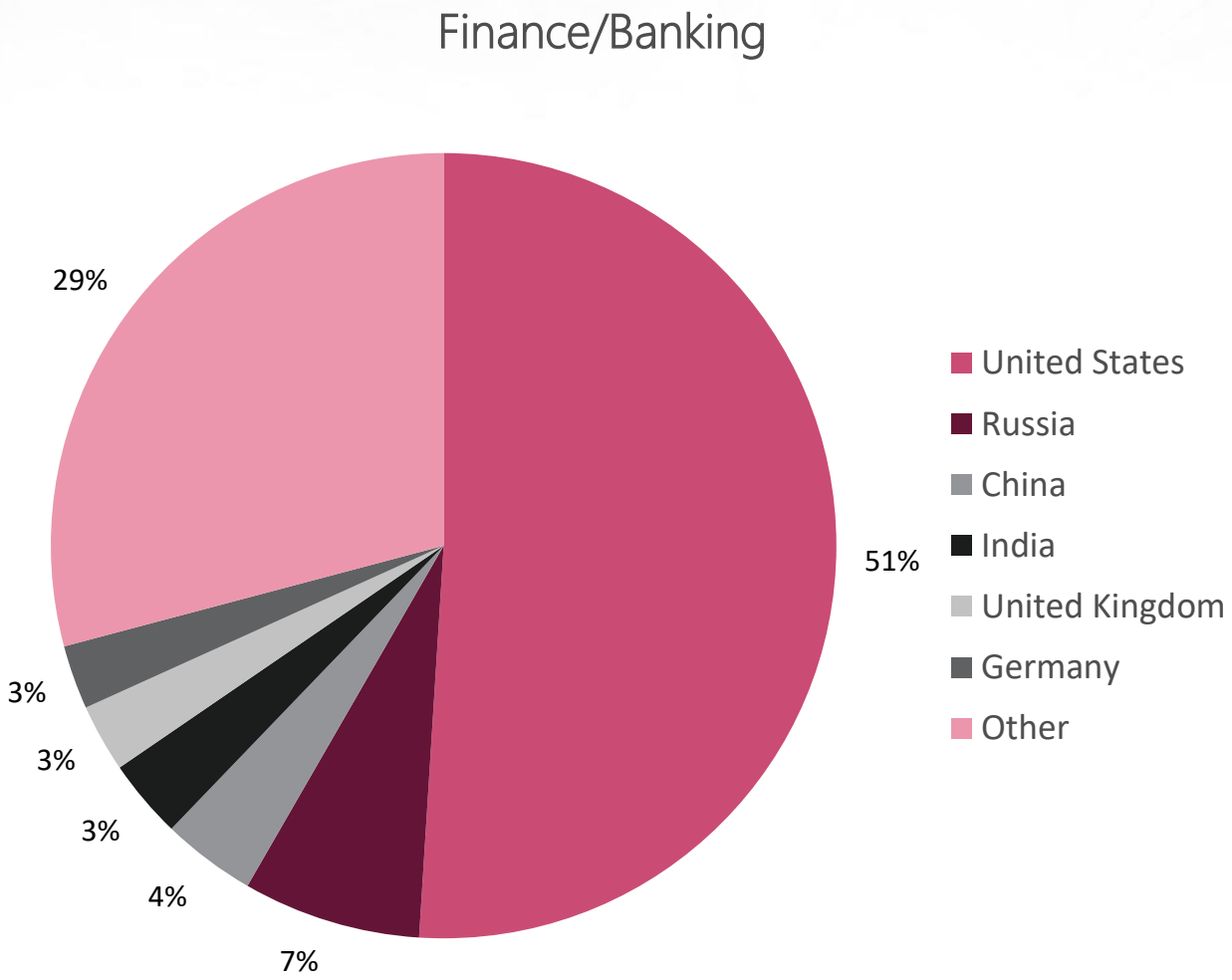
Major attacks and data breaches - Finance/Banking (Global)

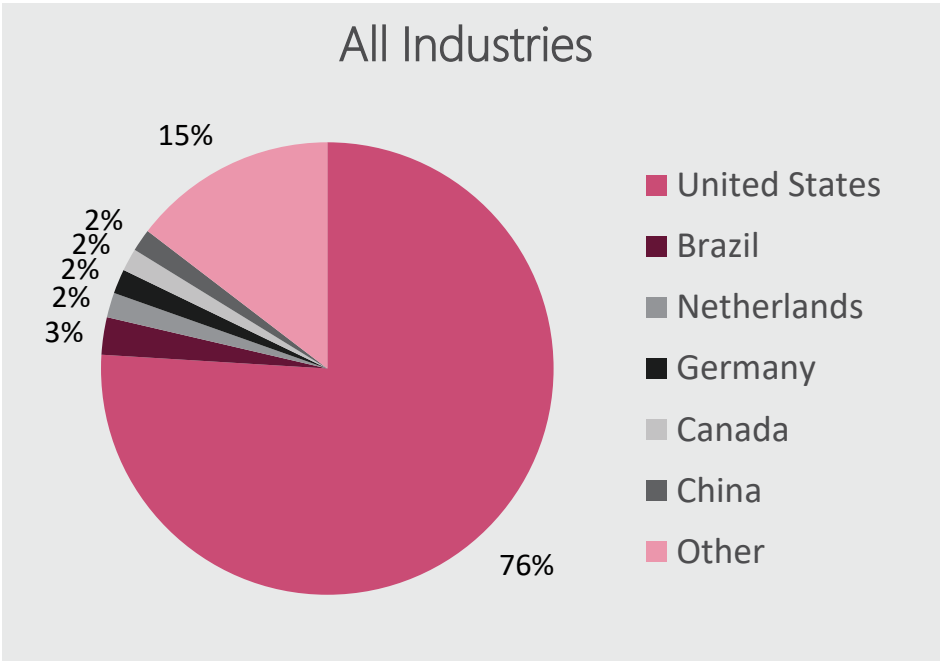
- Mar-22 - Check Point Research has analyzed the Conti Ransomware gangs chat leaks and revealed insights on the groups Hi-tech company type of management, with physical offices, HR & finance departments and more. CPR published a detailed connection map exposing the organizational structure within the key members and affiliates of the group.
- Jan-22 - Hackers have stolen $80 million worth of crypto assets from the DeFi finance platform Qubit Finance. Threat actors then contacted the company and proposed to return the stolen amount in exchange for the maximum bug bounty.
- Jan-22 - The Central Bank of Indonesia has announced that their networks were hit by a ransomware attack last month. Threat actors stole non-critical data concerning the Banks employees before encrypting the systems. The Conti gang has claimed the attack after leaking part of the allegedly stolen files.
- Dec-21 - The Anubis banking Trojan is being leveraged in cybercrime campaign impersonating the French telecommunication provider Orange. The malware can extract finance related data and more from the victims device after encouraging them to disable Google Play Protected.
- Nov-21 - Android Banking malware BrazKing makes a comeback with an upgrade including dynamic banking overlays and a new implementation trick that enables it to operate without requesting risky permissions. The malware is likely operated by a Brazilian threat group and is targeting local mobile banking users.
- Nov-21 - A new Android malware known as MasterFred is using fake Apps looking similar to Instagram, Netflix and Twitter to steal the credit card information of users.

Attacks per Organization - Americas, Last 6 Months

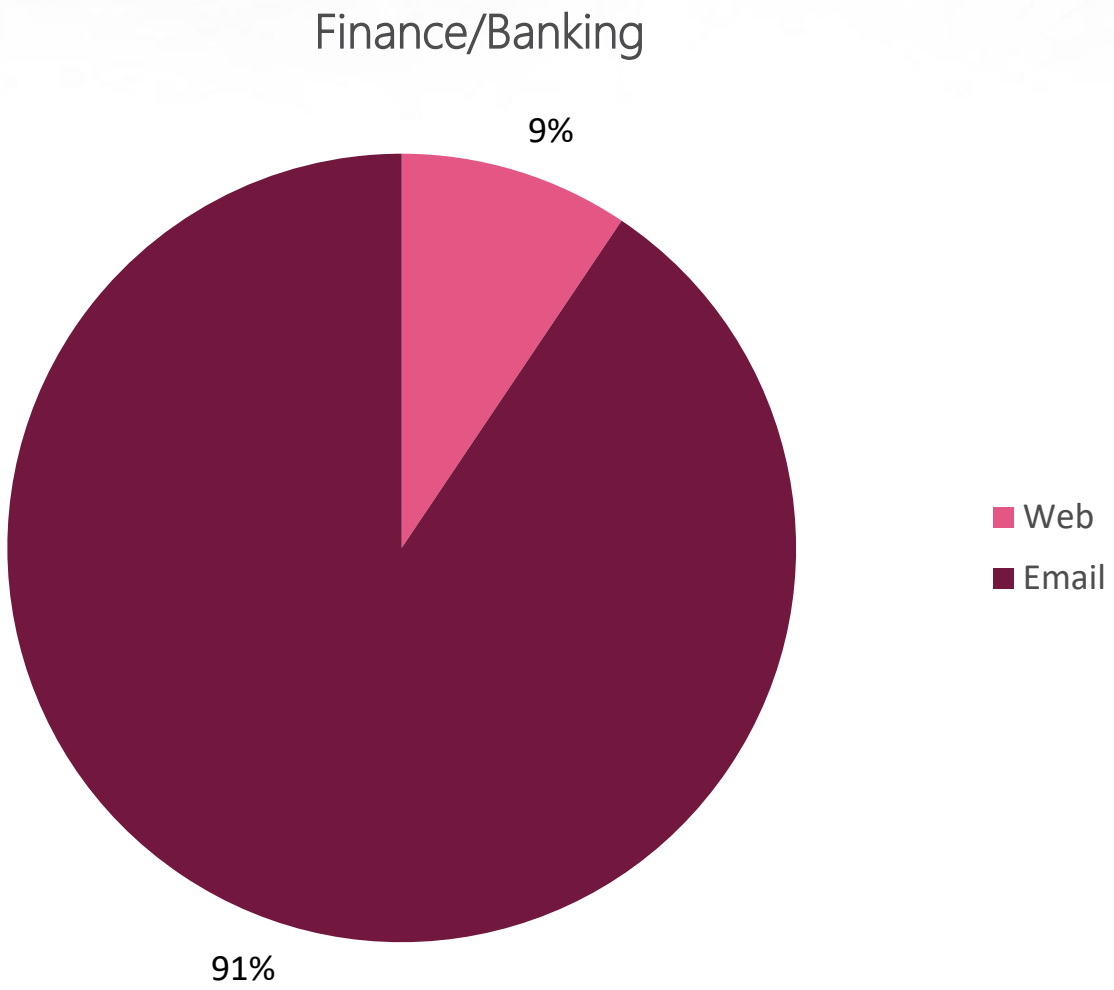


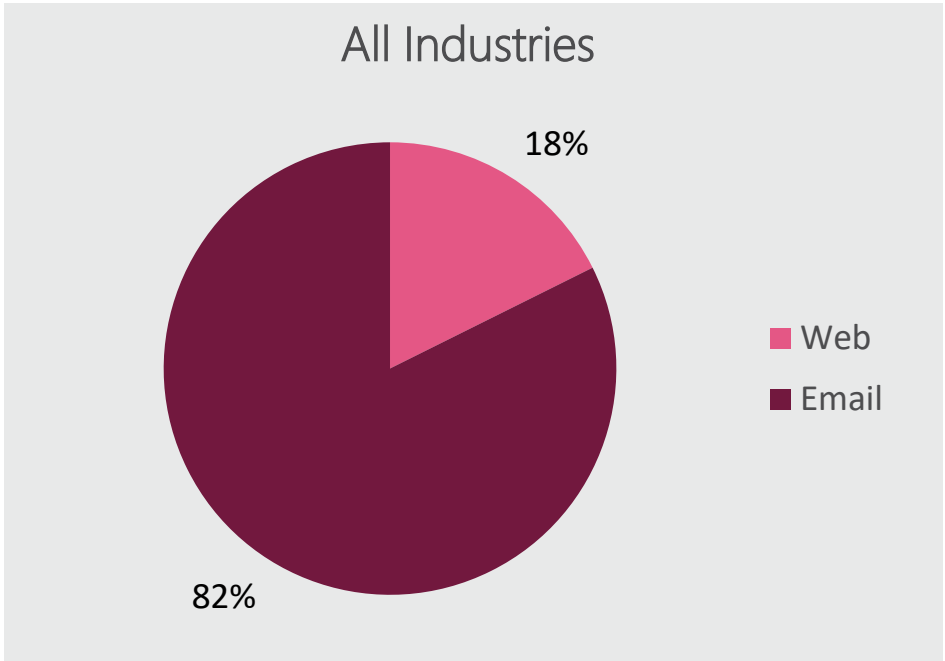
Top Threat Source Countries- Americas, Last 6 Months



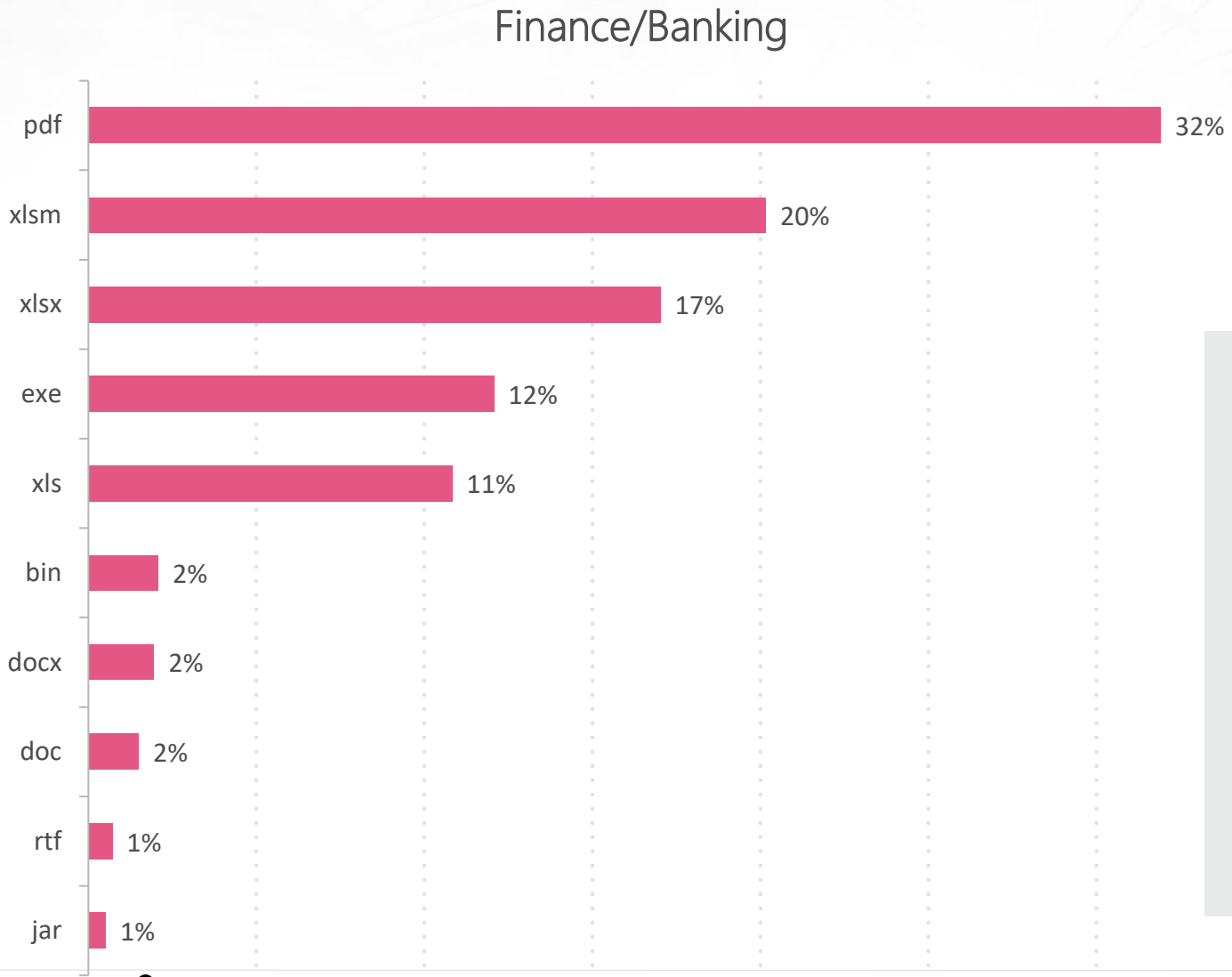


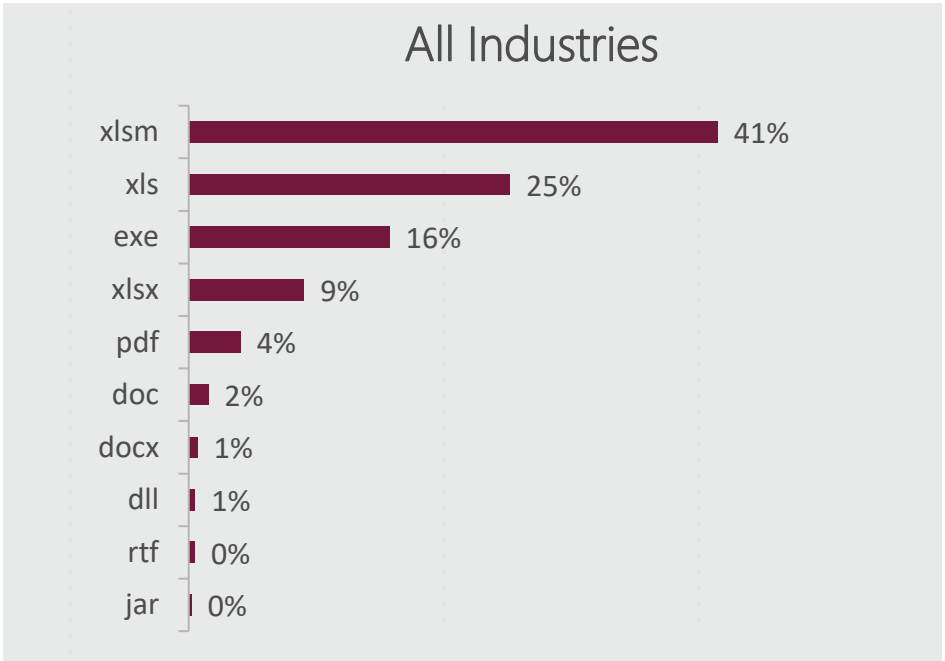
Attack Vectors for Malicious Files in Americas- Last 30 Days



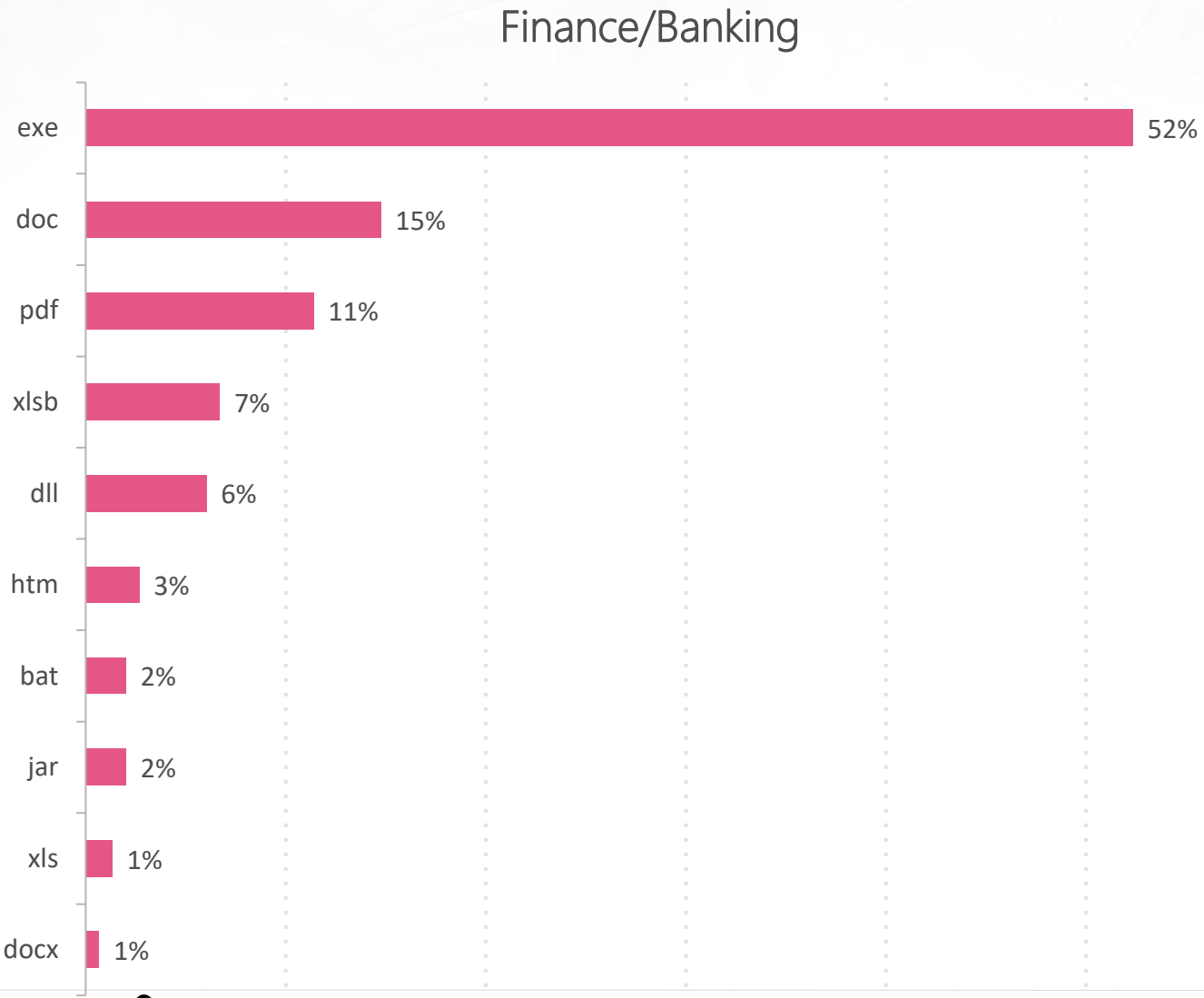


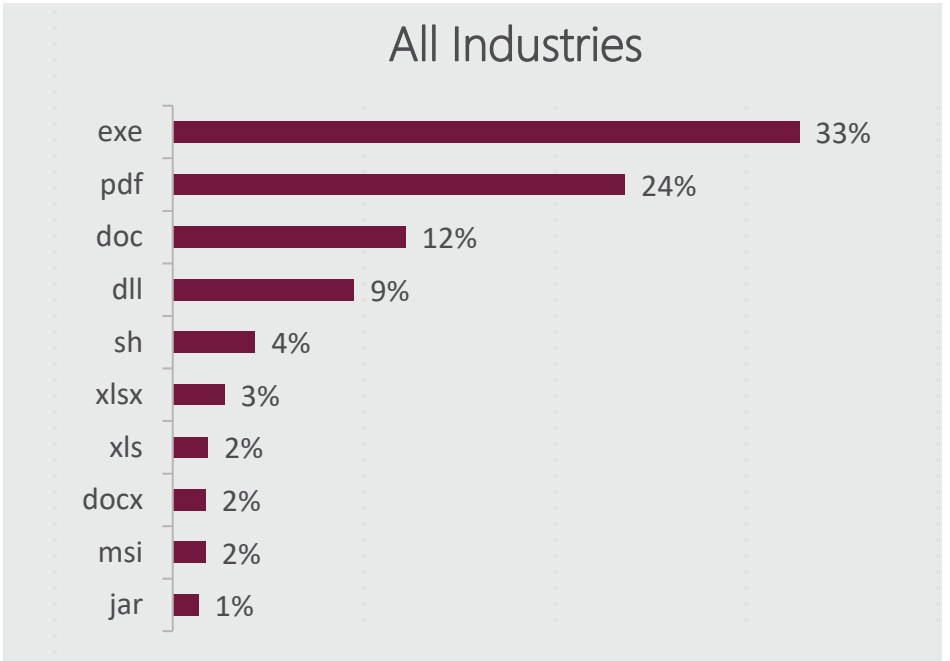
Top Malicious File Types, Email- Americas, Last 30 Days





Top Malicious File Types, Web- Americas, Last 30 Days

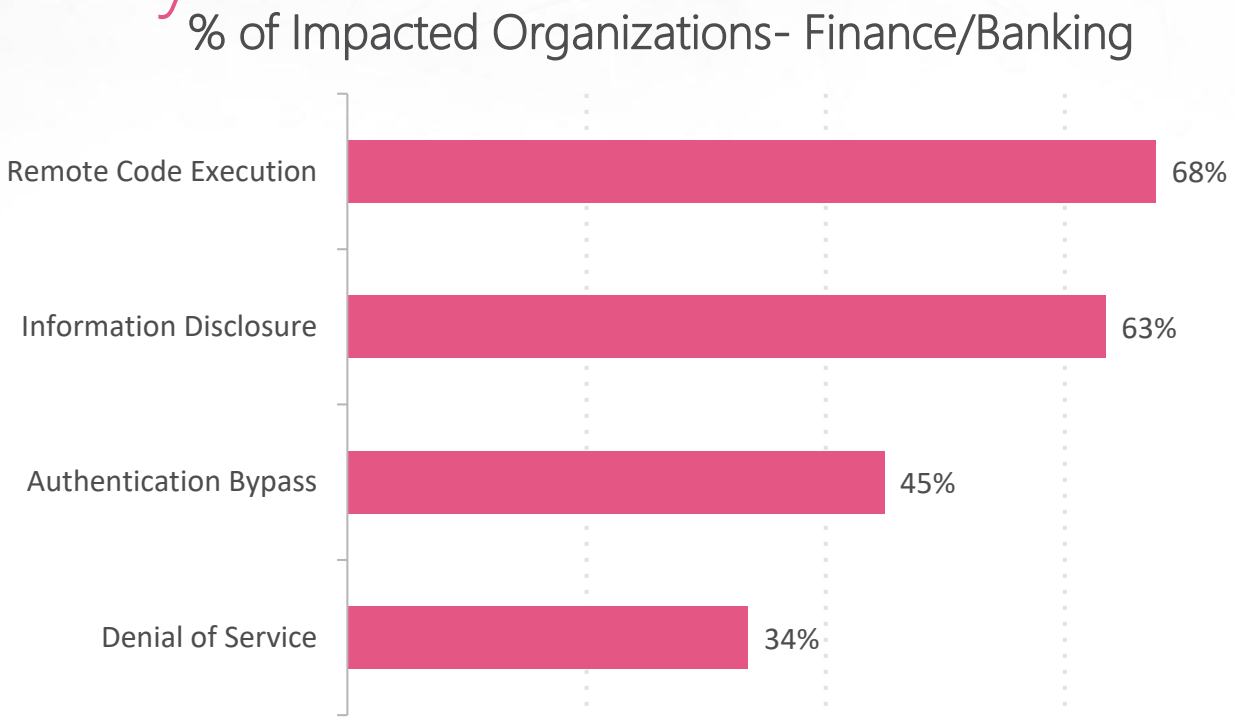


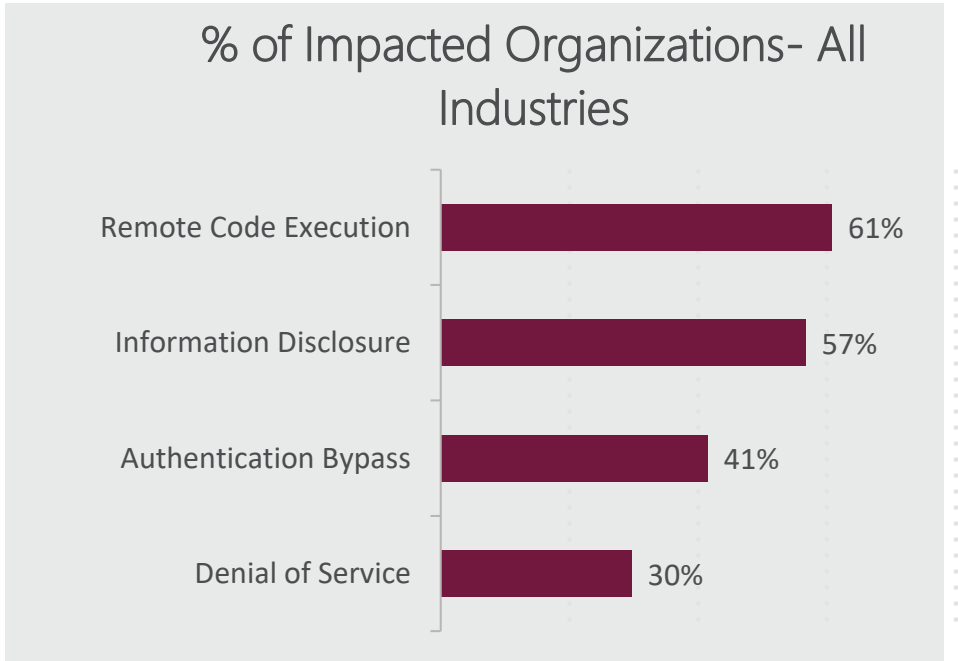


Top MITRE Techniques, Malicious EXE Files- Americas, Last 30 Days

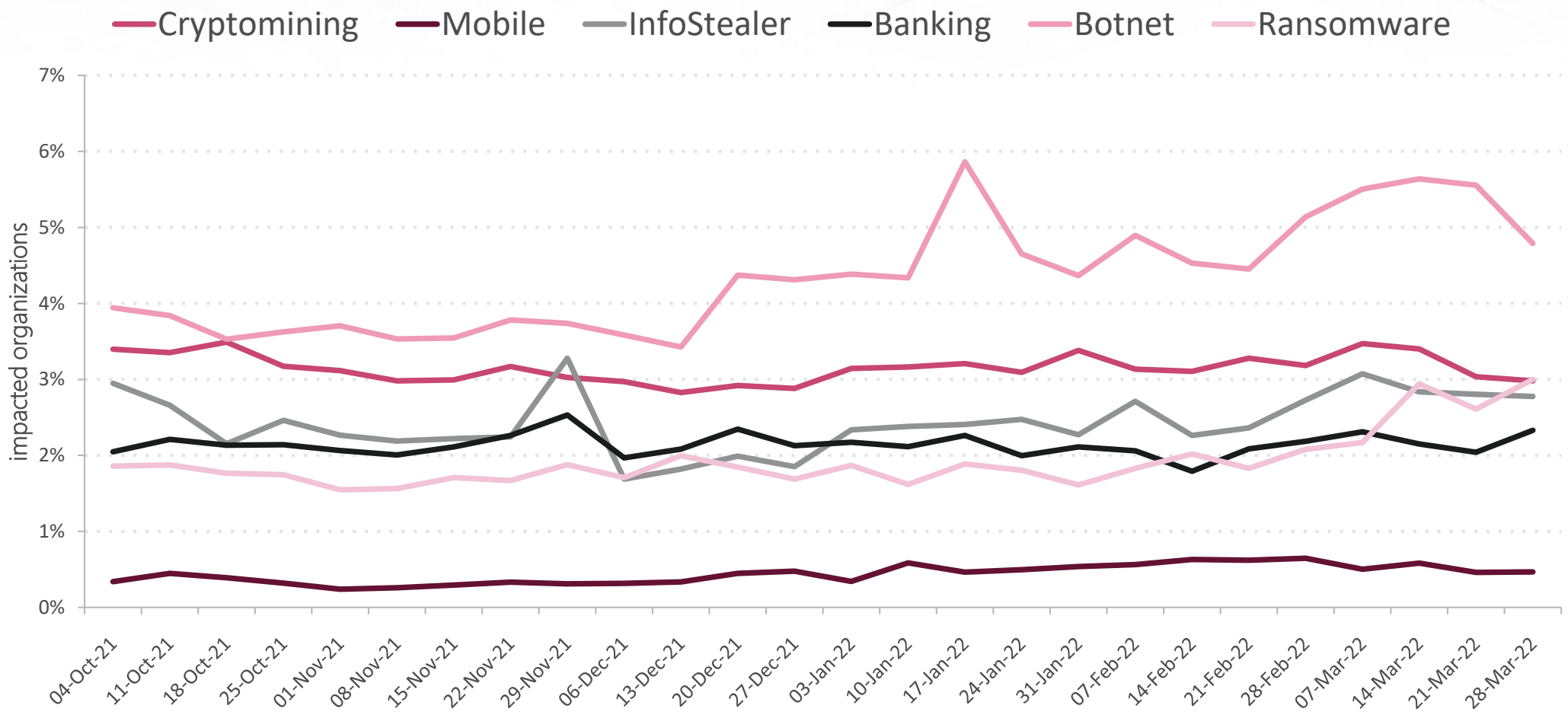
TECHNIQUE	RELATED TACTICS	FINANCE/BANKING IMPACT	ALL INDUSTRIES IMPACT
Execution through API	Execution	42%	52%
System Information Discovery	Discovery	31%	43%
Virtualization / Sandbox Evasion	Defense Evasion, Discovery	31%	44%
Data Encrypted	Exfiltration	24%	33%
File Deletion	Defense Evasion	23%	35%

Top Vulnerability Exploit types - Americas, Last 30 Days

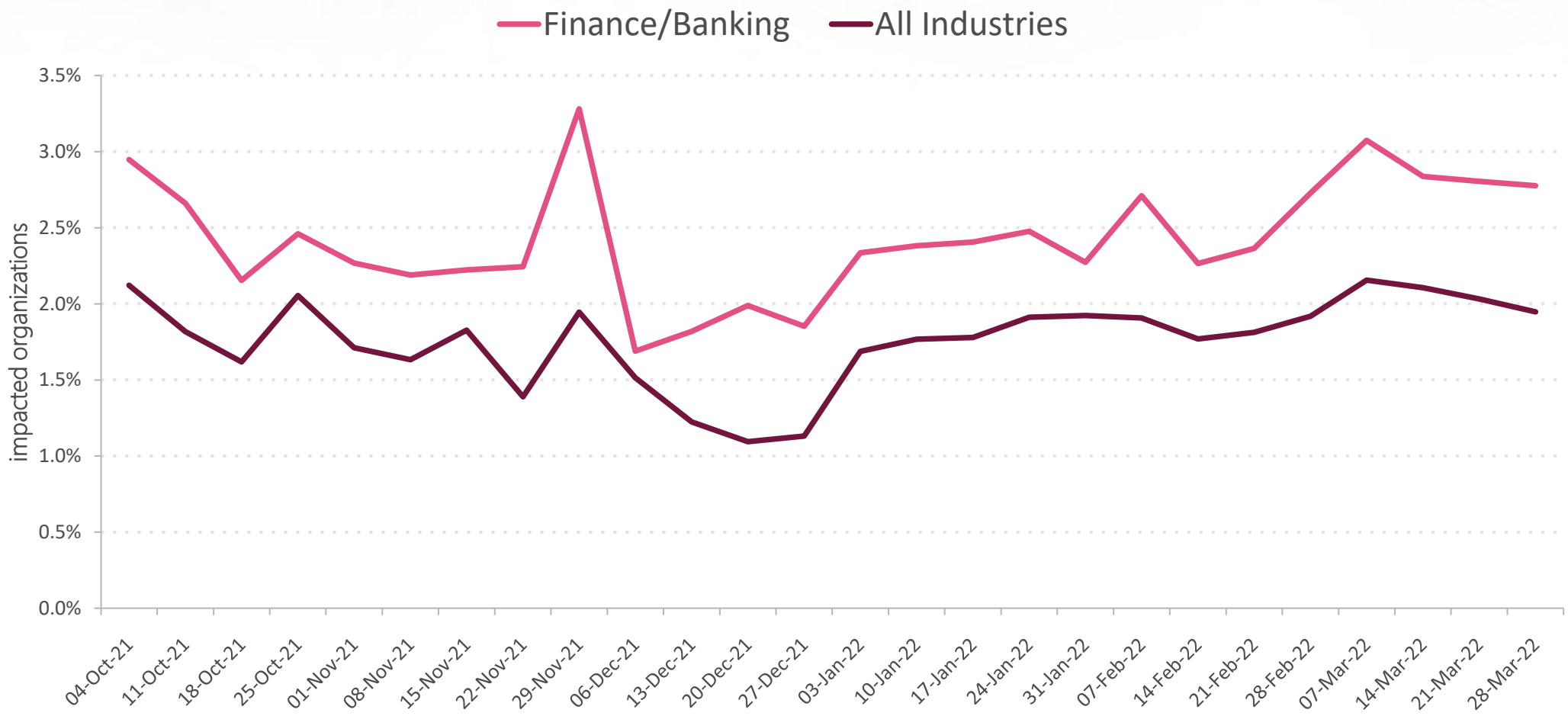




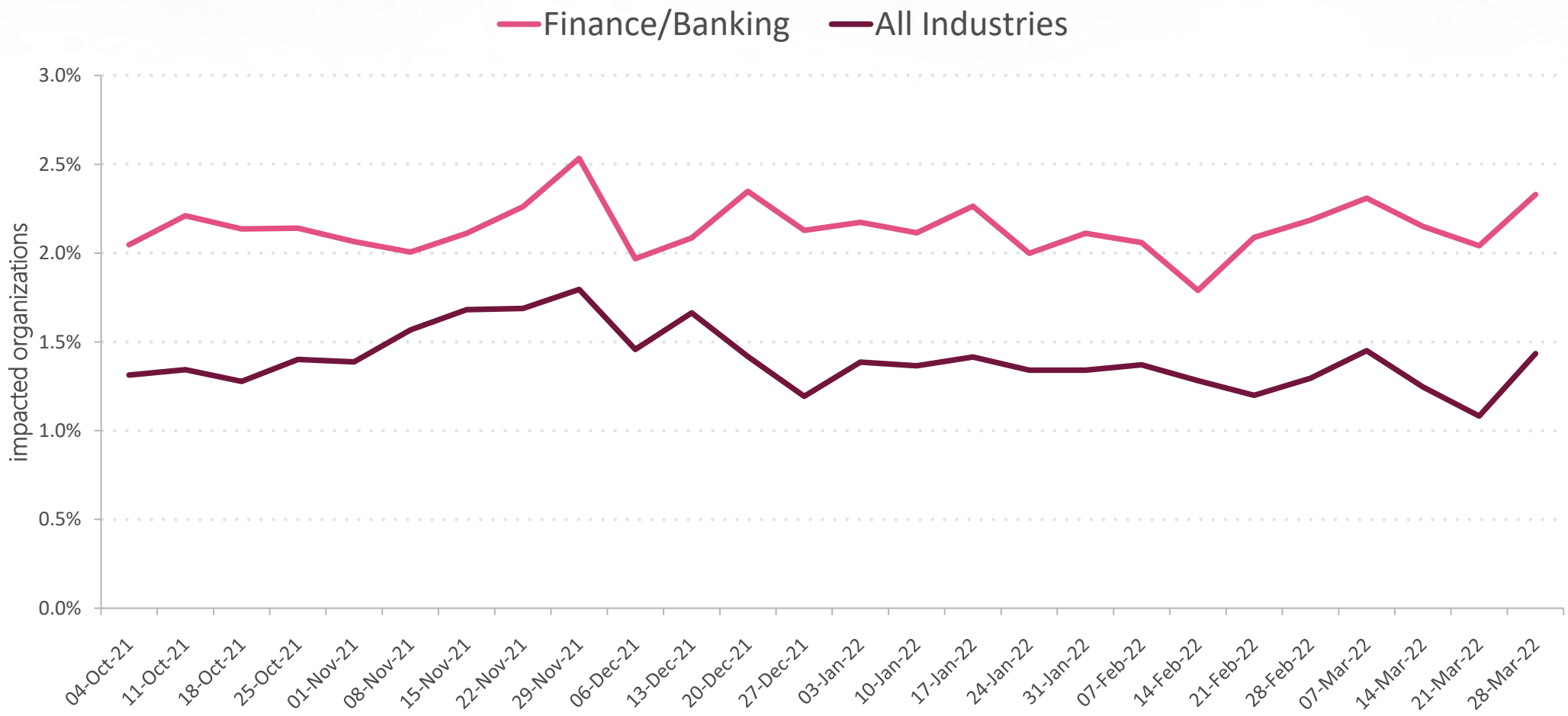
Major Malware Types trend - Americas, Last 6 Months



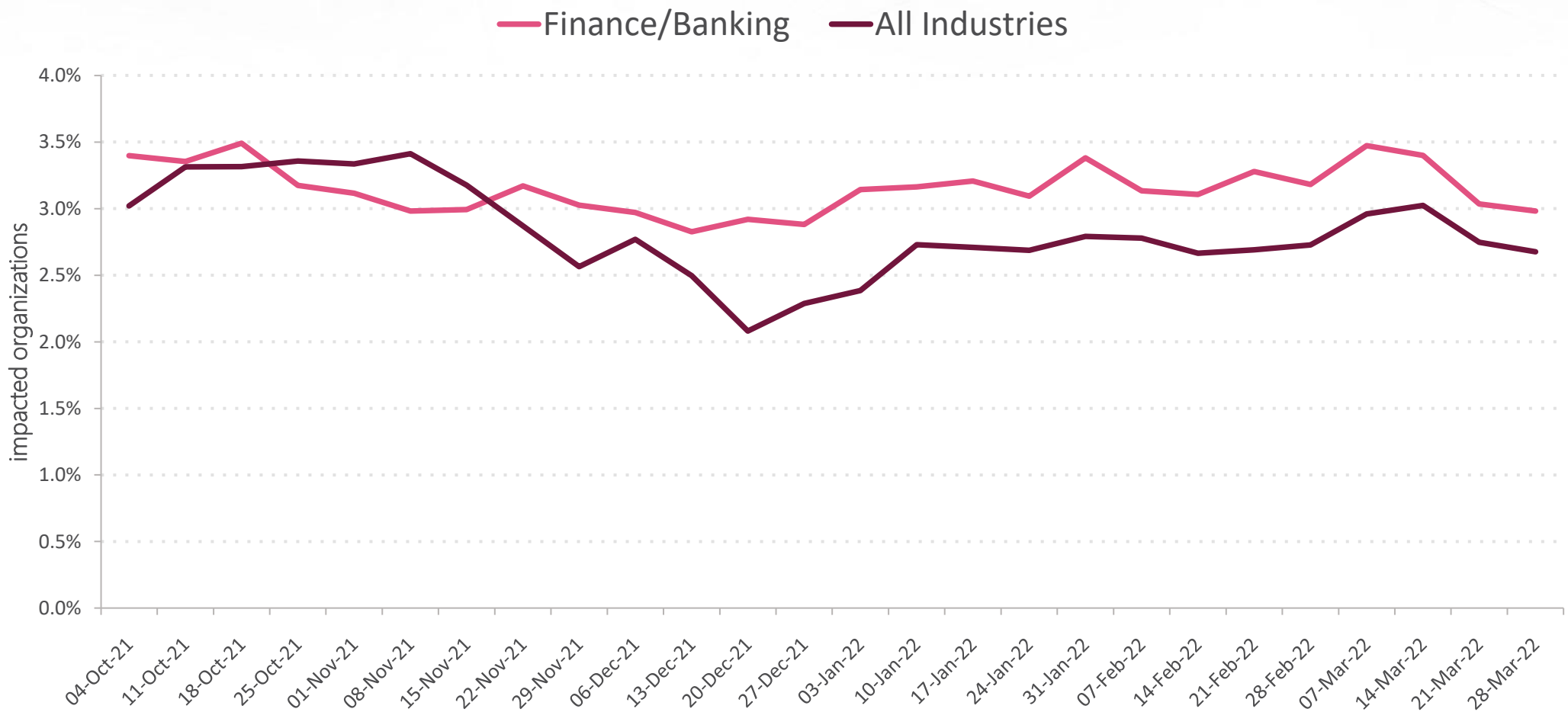
InfoStealer Attacks- Americas, Last 6 Months



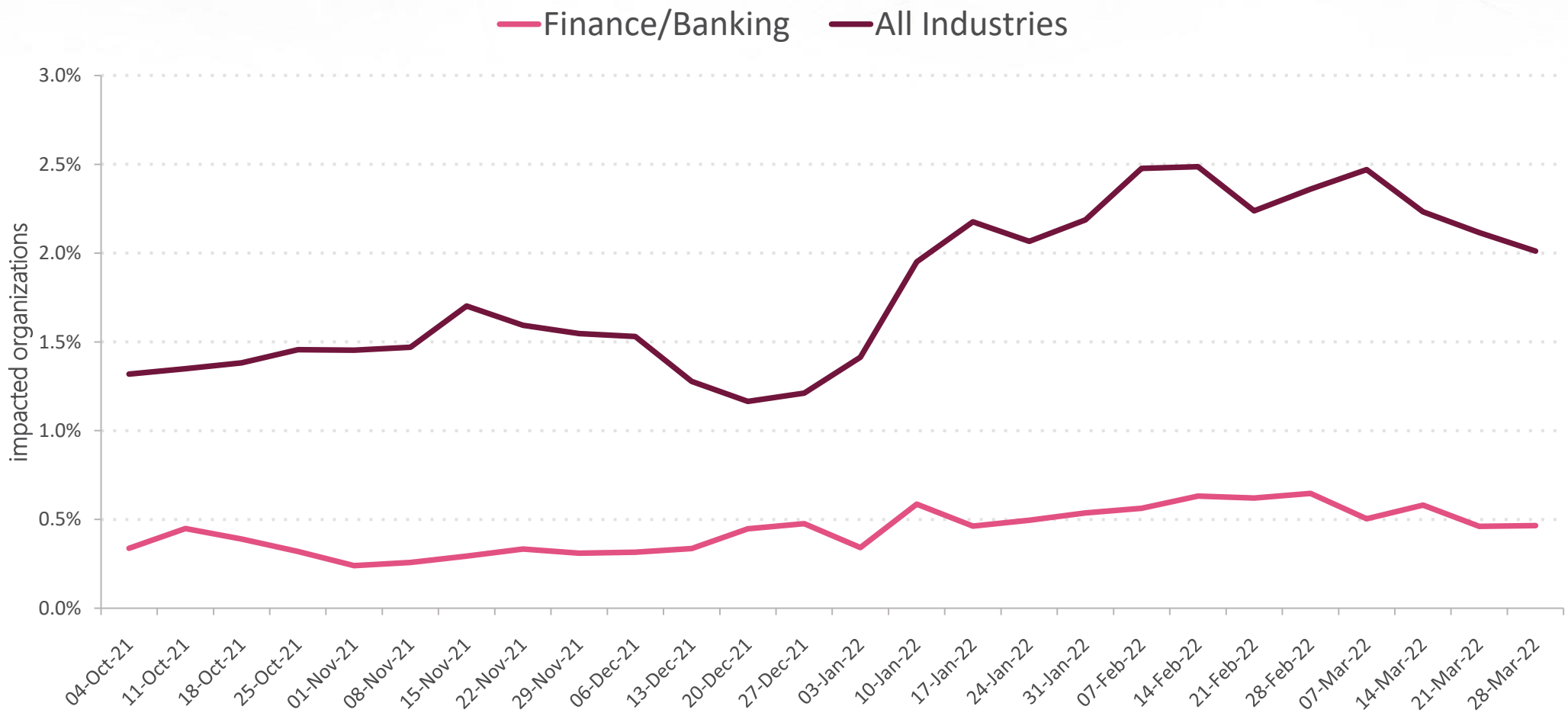
Banking Attacks- Americas, Last 6 Months



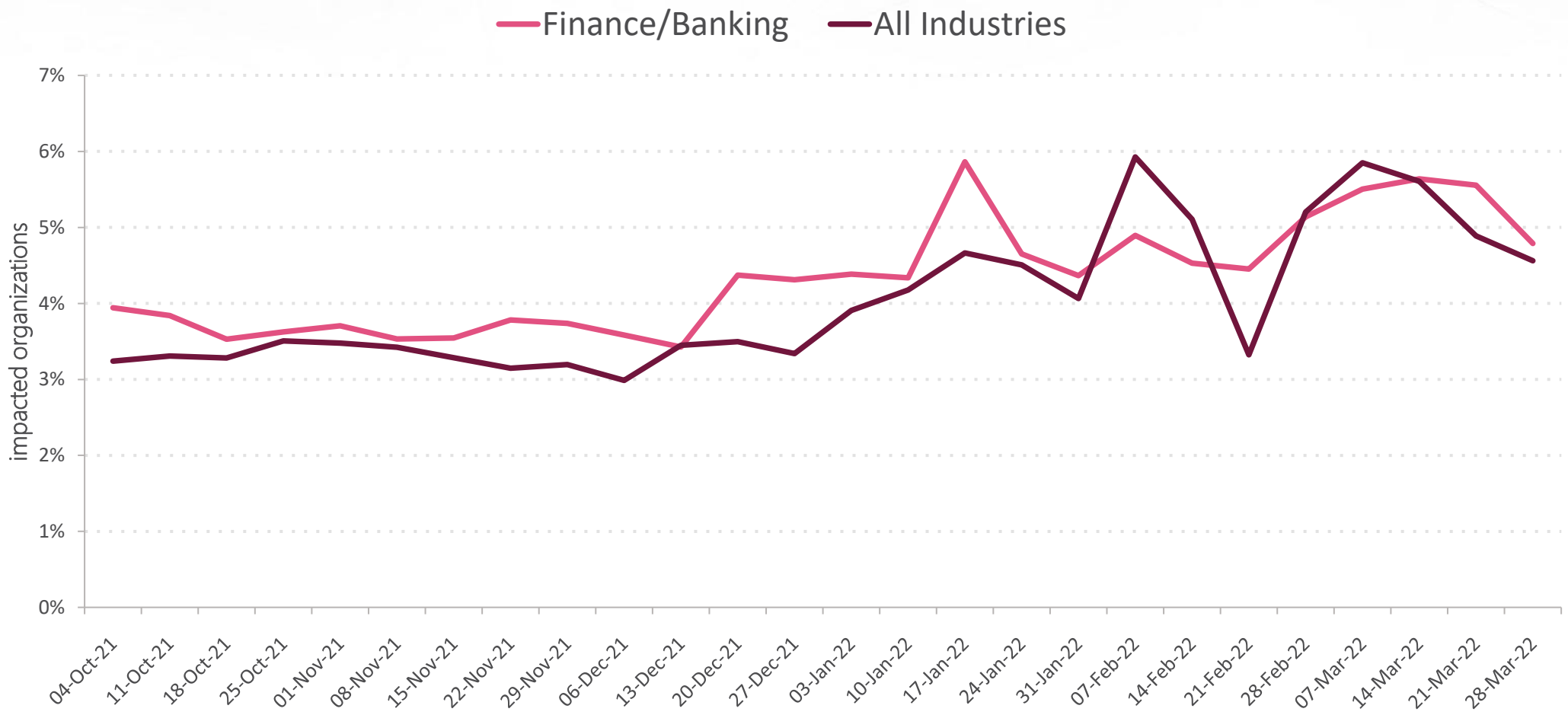
Cryptominer Attacks- Americas, Last 6 Months



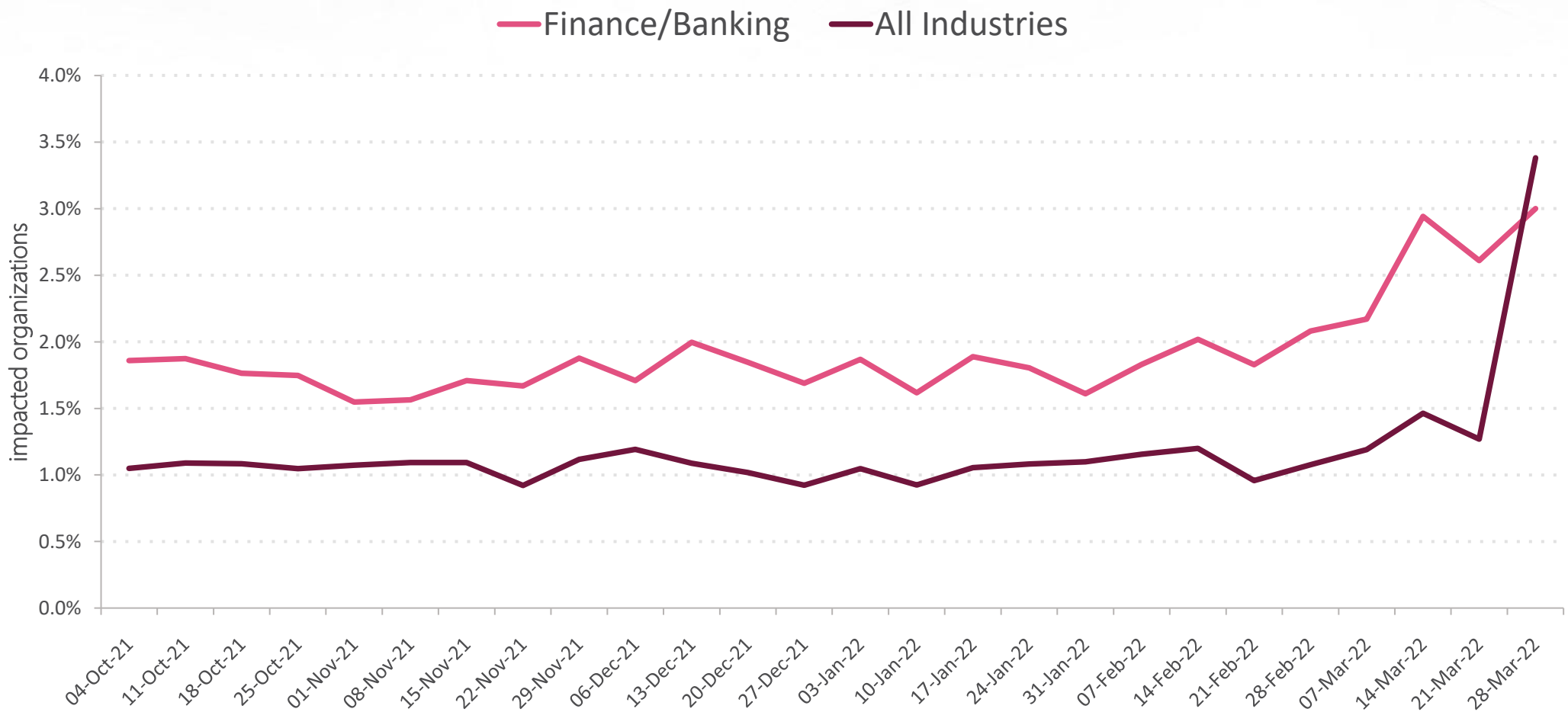
Mobile Attacks- Americas, Last 6 Months



Botnet Attacks- Americas, Last 6 Months



Ransomware Attacks- Americas, Last 6 Months




CHECK POINT
YOU DESERVE THE BEST SECURITY
THANK YOU
More Info:
https://research.checkpoint.com/
cp<r>
CHECK POINT RESEARCH