Check Point
SOFTWARE TECHNOLOGIES LTD

THREAT INTELLIGENCE REPORT

Namibia

COMPLETE ENTERPRISE SOLUTIONS

Infrastructure
Communication
Security

Check Point PARTNER

Check Point Partner CCSP

Check Point Partner MSP

cp<r>
CHECK POINT RESEARCH

Threat Intelligence Summary

- An organization in Namibia is being attacked on average 1036 times per week in the last 6 months, compared to 726 attacks per organization globally.
- The top malware in Namibia is Trickbot, impacting 13% of organizations.
- The top malware list in Namibia includes 2 Banking Trojans and 1 Trojan (Formbook).
- 50% of the malicious files in Namibia were delivered via Web.
- The most common vulnerability exploit type in Namibia is Remote Code Execution, impacting 59% of the organizations.
- Weekly impacted organizations by malware types:

	Cryptominer	Ransomware	Mobile	InfoStealer	Banking	Botnet
Namibia Avg.	1.7%	2.3%	0.8%	0.6%	3.8%	9.9%
Global Avg.	3.8%	2.1%	1.2%	1.8%	5.1%	10.0%

- View the latest publications by Check Point Research

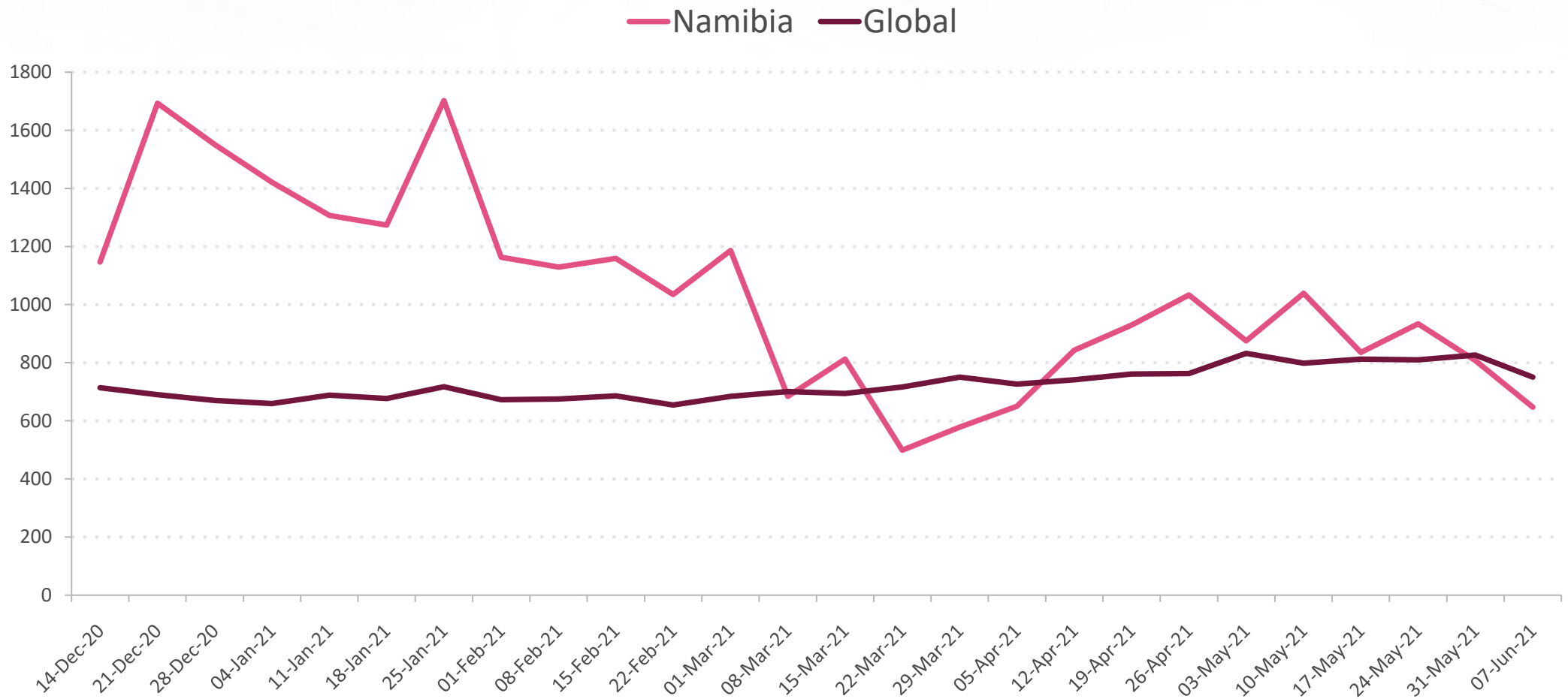
Threat Landscape

- **Cloud adoption races ahead of security -** 2020 saw organizations' digital transformation programs advance by over five years in response to the pandemic, but public cloud security is still a major concern for 75% of enterprises. Also, over 80% of enterprises found their existing security tools don't work at all or have only limited functions in the cloud, showing that cloud security problems will continue into 2021.
- **Remote working is targeted -** Hackers ramped up 'thread hijacking' attacks on remote workers to steal data or infiltrate networks using the Emotet and Qbot trojans, which impacted 24% of organizations globally. Attacks against remote access systems such as RDP and VPN also increased sharply.
- **Double-extortion ransomware attacks rise -** In Q3 2020, nearly half of all ransomware incidents involved the threat of releasing data stolen from the target organization. On average, a new organization becomes a victim of ransomware every 10 seconds worldwide.
- **Attacks on healthcare sector become an epidemic -** In Q4 2020, CPR reported that cyber-attacks (especially ransomware attacks) on hospitals had increased by 45% worldwide, because criminals believe they are more likely to meet ransom demands due to the pressures from COVID-19 cases.
- **Mobiles are moving targets -** 46% of organizations had at least one employee download a malicious mobile application, which threatens their networks and data in 2020. The increased use of mobiles during global lockdowns has also driven growth in banking and information-stealing mobile Trojans.
- For more data and examples please see Check Point Research Cyber Attack Trends: 2021 Annual Report.

Major attacks and data breaches- Global- Last Month

- A spear-phishing campaign has been targeting travel and aerospace companies utilizing two RATs, RevengeRAT and AsyncRAT, deployed via a newly exposed malware loader. Spoofed email addresses are used in the phishing emails, as well as images posing as PDF files.
- Ireland's Health Services Executive (HSE), a provider of health and social services, among them Covid-19 vaccines, has suffered an attack by Conti ransomware, forcing it to shut down its IT systems. Vaccine appointments have not been affected, however other hospital services might be affected.
- Rapid7 Cybersecurity Company has disclosed that parts of its source code, as well as data of its MDR customers, have been accessed by threat actors as part of the Codecov supply chain attack.
- Reporters claim that Colonial Pipeline has paid a $5 million ransom. Researchers have determined that the DarkSide ransomware criminal group, probably from Russian origins, are behind the attack, rather than Russian state-sponsored groups. In parallel, the DarkSide gang announced it is shutting down its operations after its servers had been seized and its cryptocurrency funds, used to pay affiliates of the ransomware-as-a-service program, had been stolen.
- The cybercrime gang FIN7, has been distributing a backdoor dubbed Lizar, disguised as a Windows pen-testing tool for ethical hackers. The group pretends to be a legitimate organization that offers an analysis tool for sale.
- Threat actors have been abusing Microsoft Build Engine, a platform used to build applications, to deliver RATs and password stealers filelessly in a currently active campaign. The malicious Microsoft Build files were embedded with executables and shellcode that deploy backdoors, enabling further information theft.

Attacks per Organization - Last 6 Months



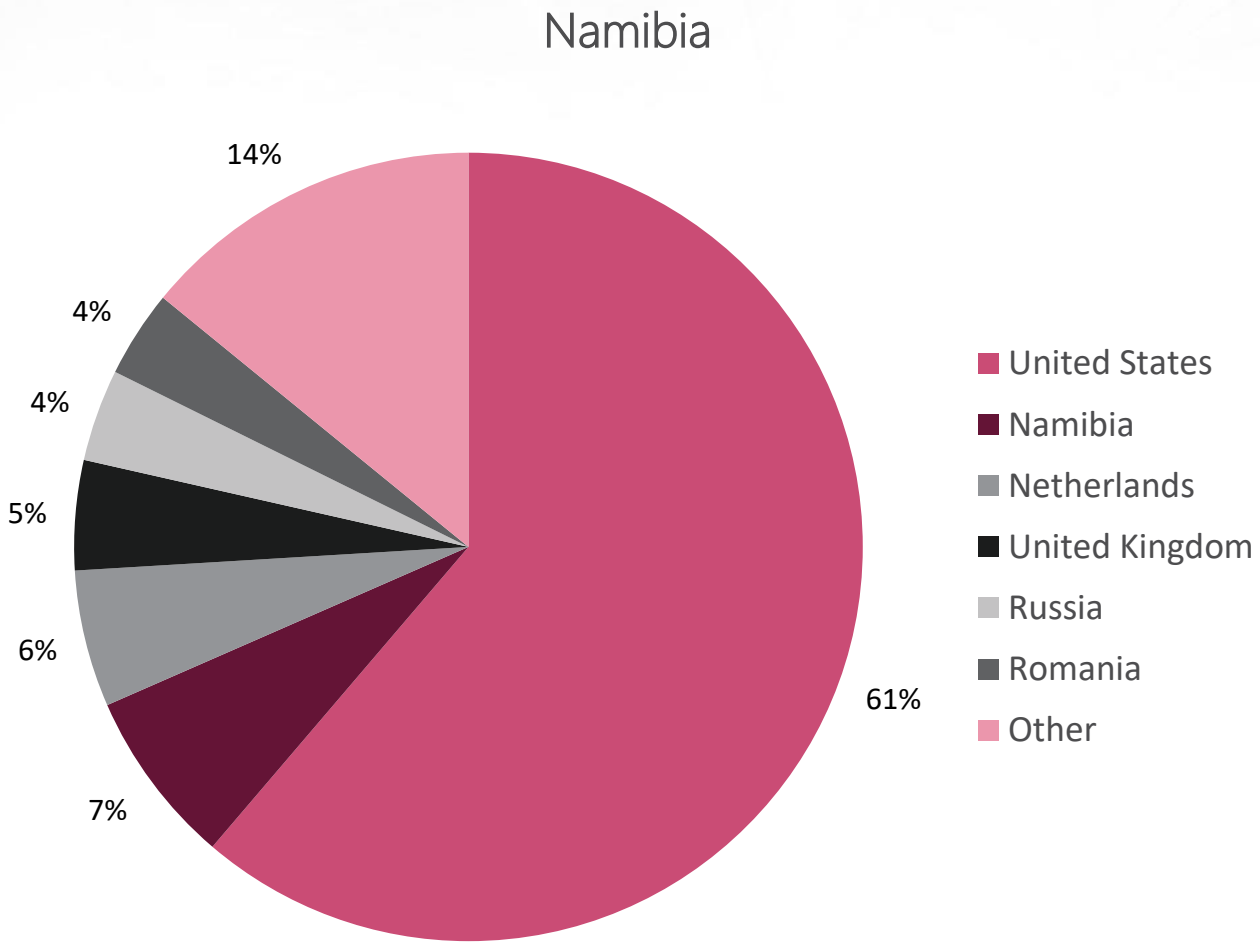
Top Malware - Namibia- May-21

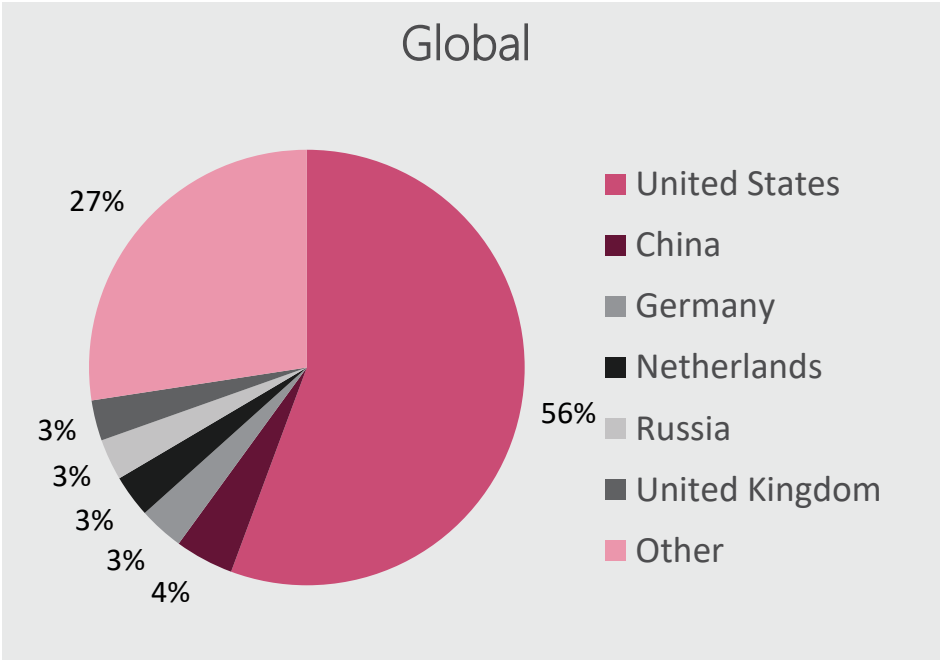
MALWARE FAMILY	NAMIBIA IMPACT	GLOBAL IMPACT	DESCRIPTION
Trickbot	13%	8%	Trickbot is a modular Botnet and Banking Trojan that targets the Windows platform, mostly delivered via spam campaigns or other malware families such as Emotet. Trickbot sends information about the infected system and can also download and execute arbitrary modules from a large array of available modules: from a VNC module for remote control, to an SMB module for spreading within a compromised network. Once a machine is infected, the Trickbot gang, 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.
Formbook	7%	3%	First detected in 2016, FormBook is an InfoStealer that targets the Windows OS. It is marketed as 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.
Dridex	3%	0%	Dridex is a Banking Trojan that targets the Windows platform, observed delivered by spam campaigns and Exploit Kits, which relies on WebInjects to intercept and redirect banking credentials to an attacker-controlled server. Dridex contacts a remote server, sends information about the infected system and can also download and execute additional modules for remote control.

Top Malware - Global- May-21

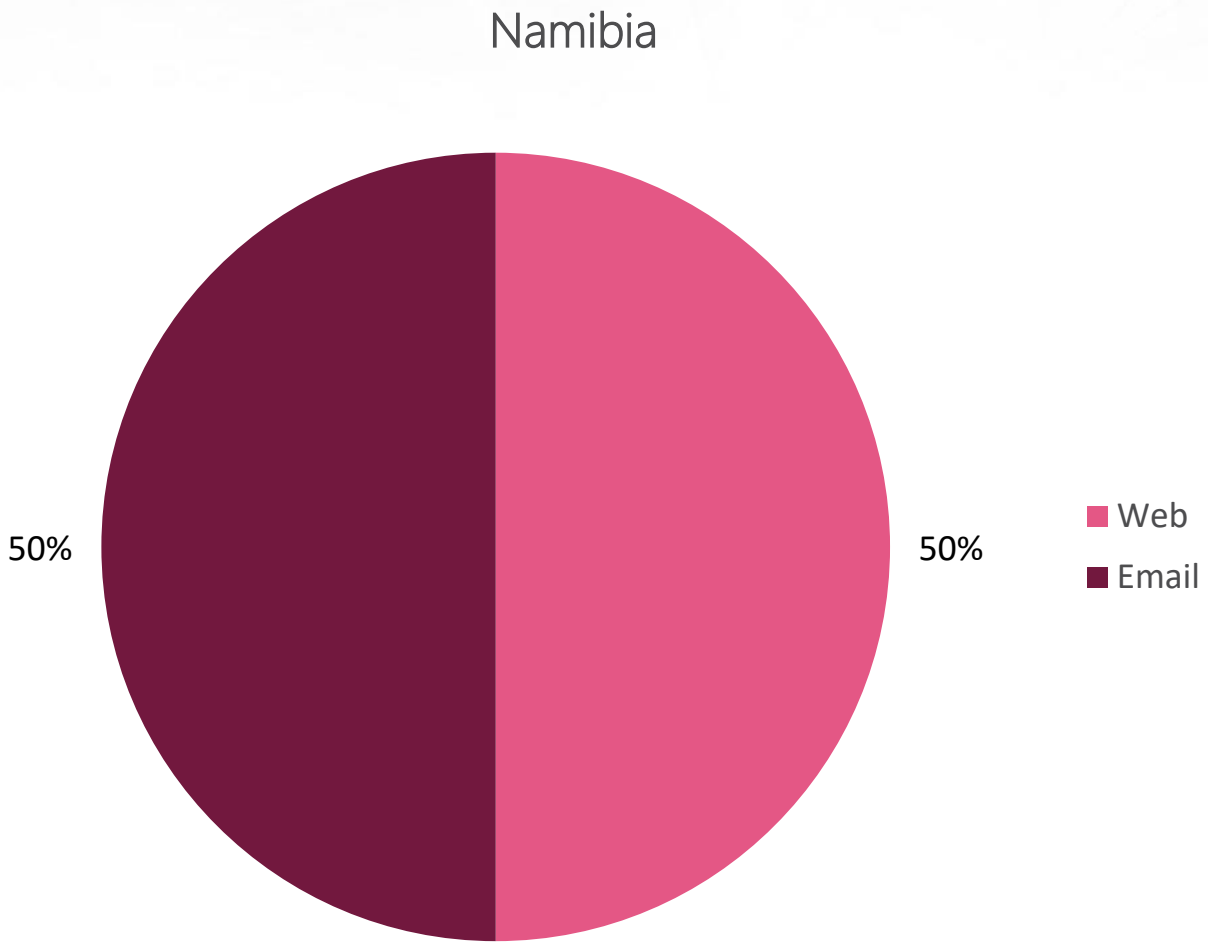
MALWARE FAMILY	GLOBAL IMPACT	DESCRIPTION
Trickbot	8%	Trickbot is a modular Botnet and Banking Trojan that targets the Windows platform, mostly delivered via spam campaigns or other malware families such as Emotet. Trickbot sends information about the infected system and can also download and execute arbitrary modules from a large array of available modules: from a VNC module for remote control, to an SMB module for spreading within a compromised network. Once a machine is infected, the Trickbot gang, 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	3%	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.
Formbook	3%	First detected in 2016, FormBook is an InfoStealer that targets the Windows OS. It is marketed as 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.
AgentTesla	2%	AgentTesla is an advanced RAT (remote access Trojan) that functions as a keylogger and password stealer. Active since 2014, AgentTesla can monitor and collect the victim's keyboard input and system clipboard, and can record screenshots and exfiltrate credentials entered for a variety of software installed on the victim's machine (including Google Chrome, Mozilla Firefox and Microsoft Outlook email client). AgentTesla is openly sold as a legitimate RAT with customers paying $15 - $69 for user licenses.
Lokibot	2%	First identified in February 2016, LokiBot is a commodity infostealer with versions for both the Windows and Android OS. It harvests credentials from a variety of applications, web browsers, email clients, IT administration tools such as PuTTY and more. LokiBot is sold on hacking forums and it is believed that its source code was leaked, thus allowing numerous variants to appear. Since late 2017, some Android versions of LokiBot include ransomware functionality in addition to their infostealing capabilities.

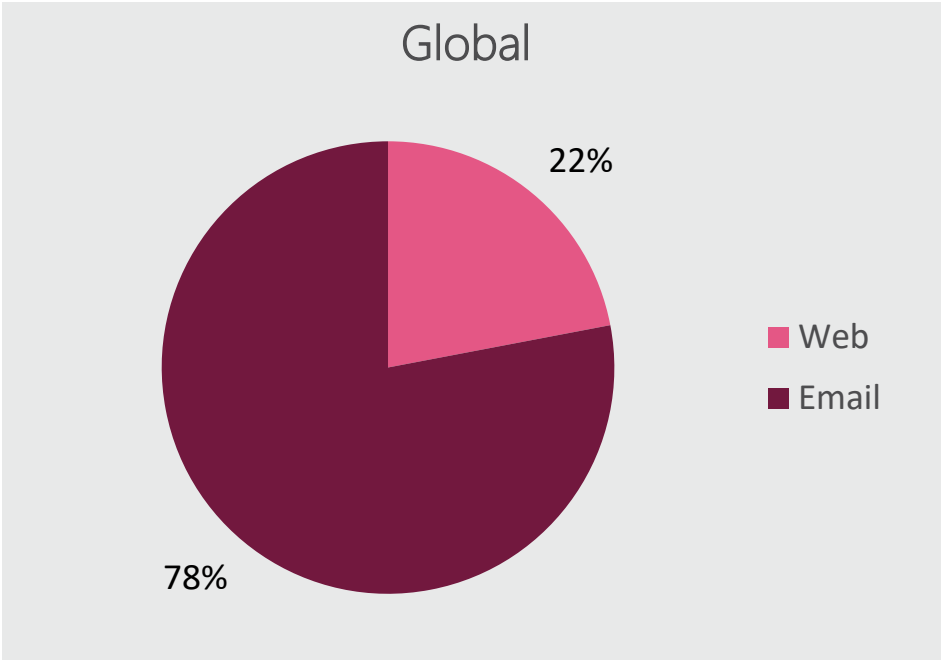
Top Threat Source Countries- Last 6 Months





Attack Vectors for Malicious Files- Last 30 Days

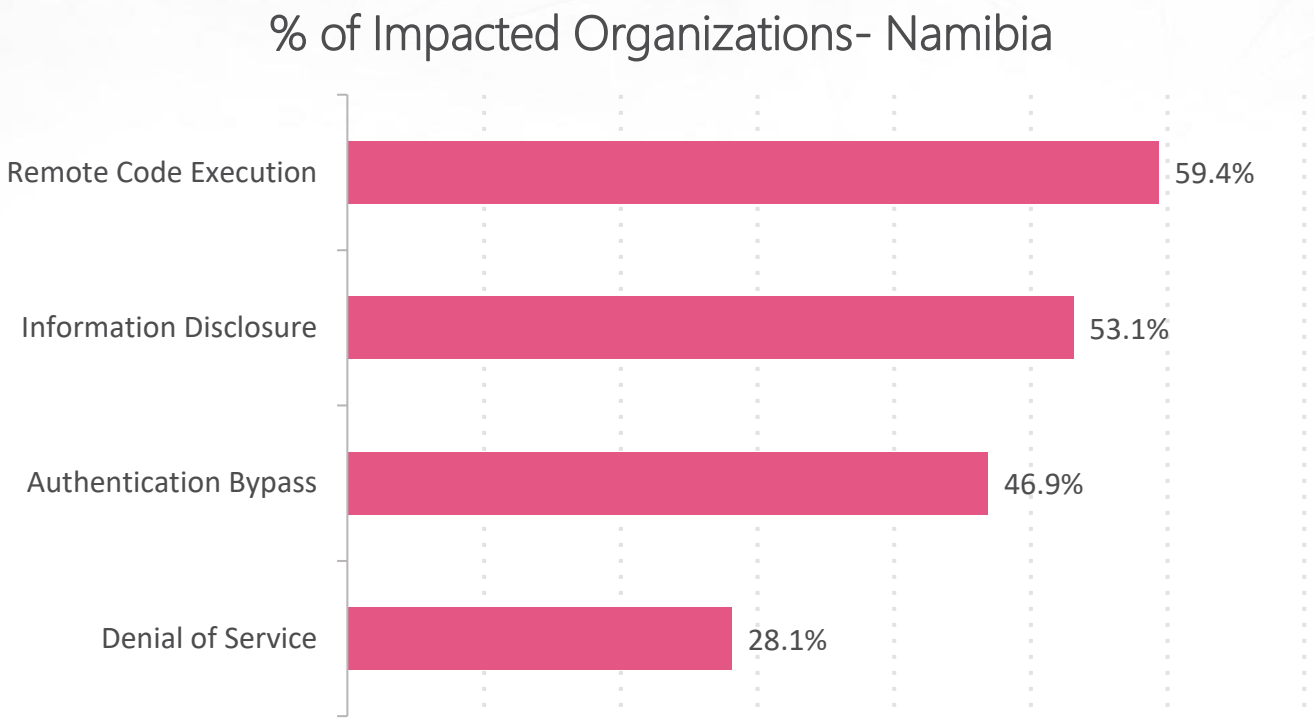


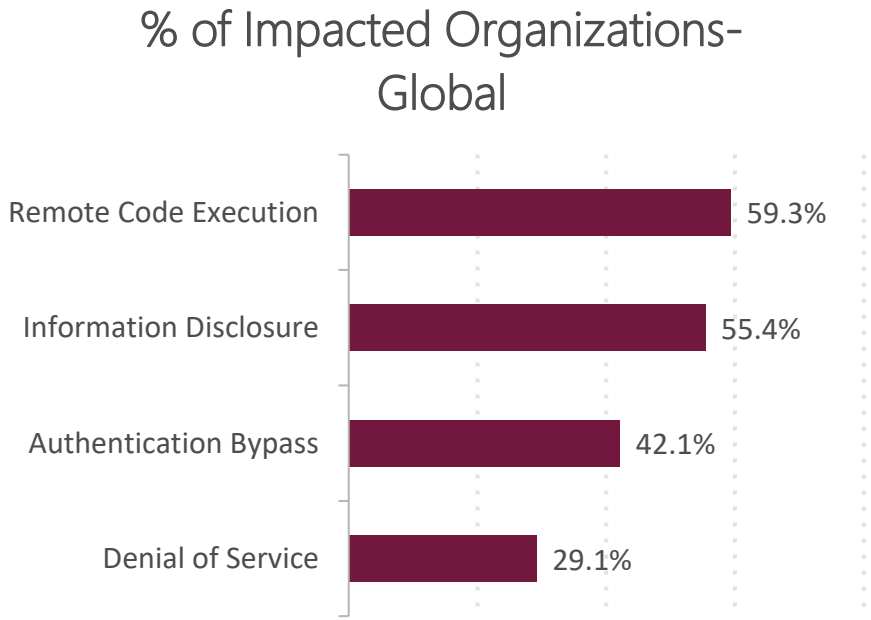


Top MITRE Techniques, Malicious EXE Files- Last 30 Days

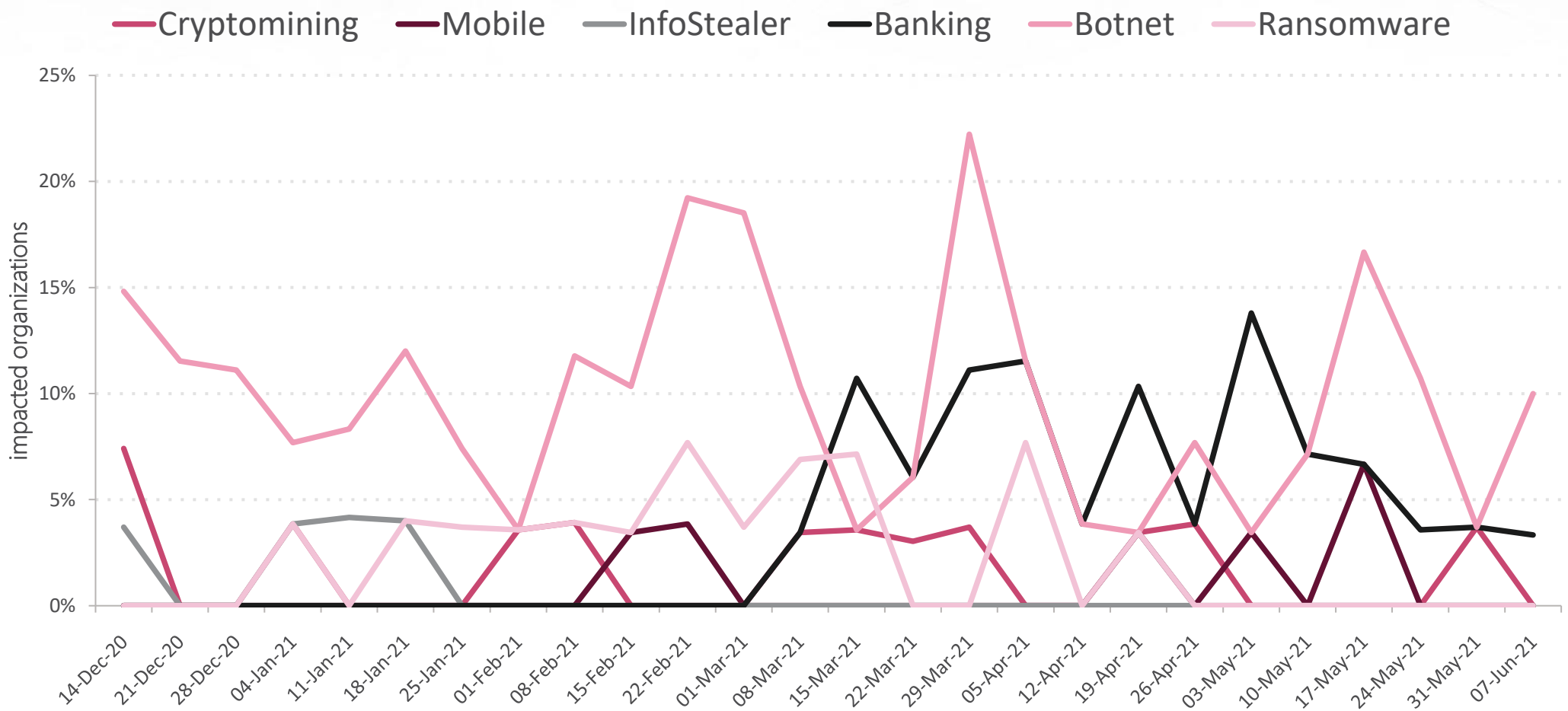
TECHNIQUE	RELATED TACTICS	NAMIBIA IMPACT	GLOBAL IMPACT
Execution through API	Execution	70%	54%
System Information Discovery	Discovery	60%	51%
Hooking	Persistence, Privilege Escalation, Credential Access	50%	25%
Data Encrypted	Exfiltration	40%	40%
Service Execution	Execution	40%	35%

Top Vulnerability Exploit types - Last 30 Days

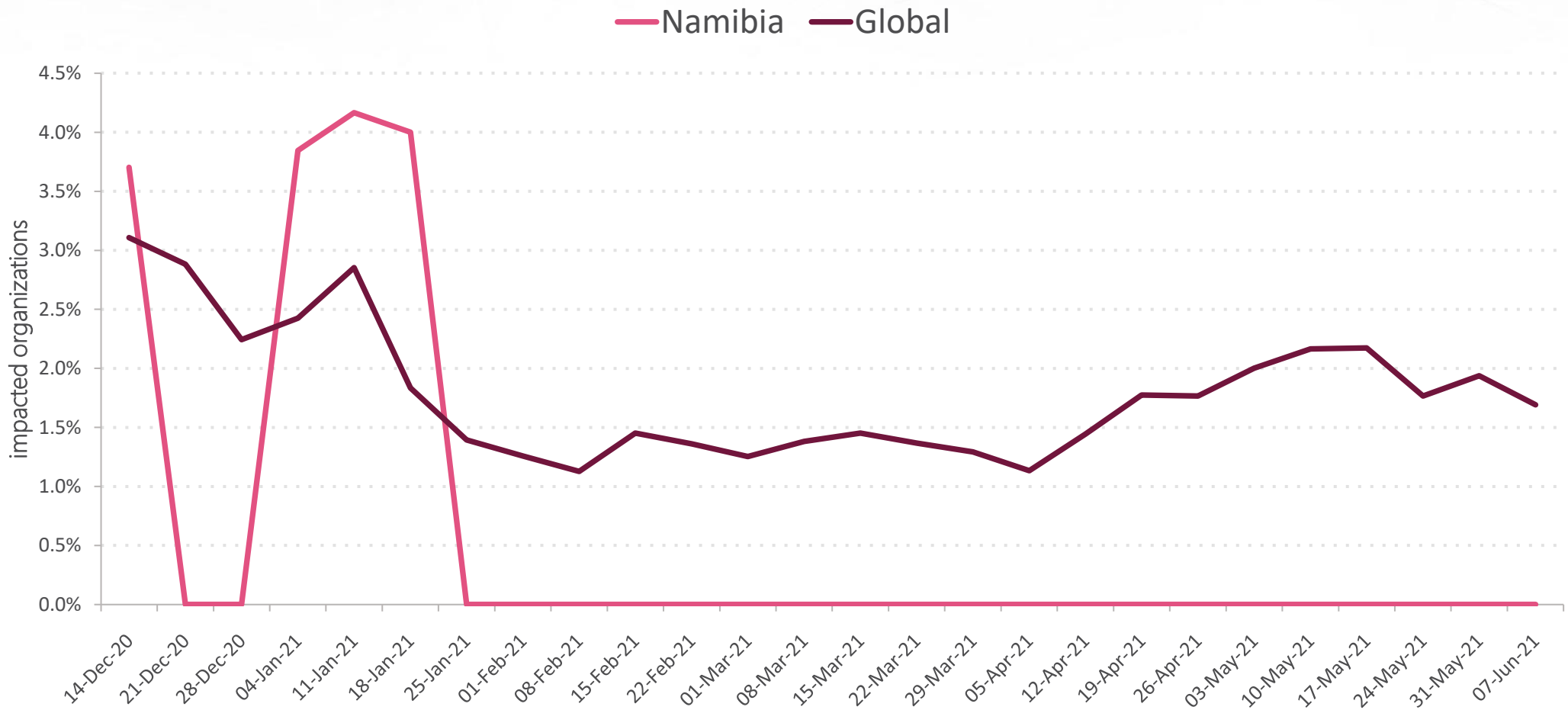




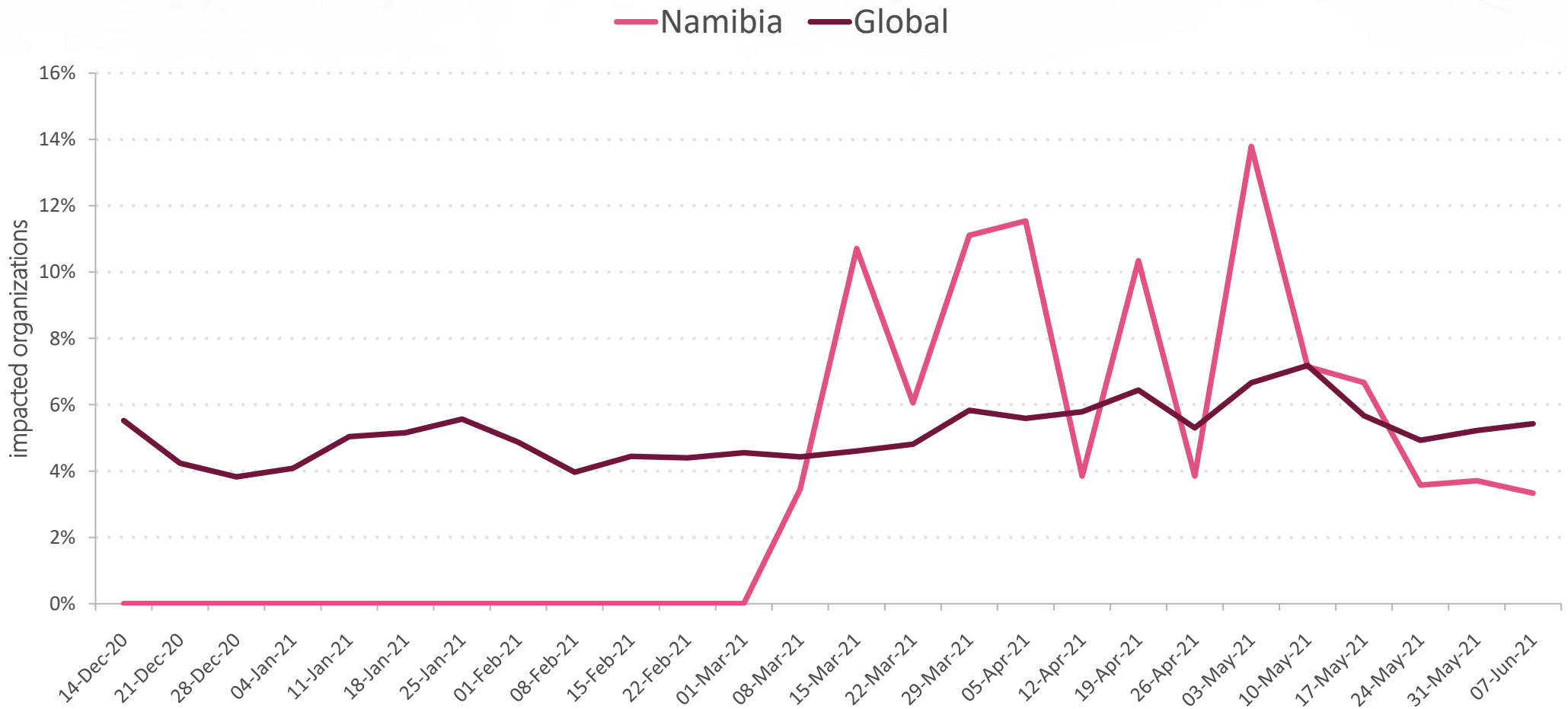
Major Malware Types trend - Namibia, Last 6 Months



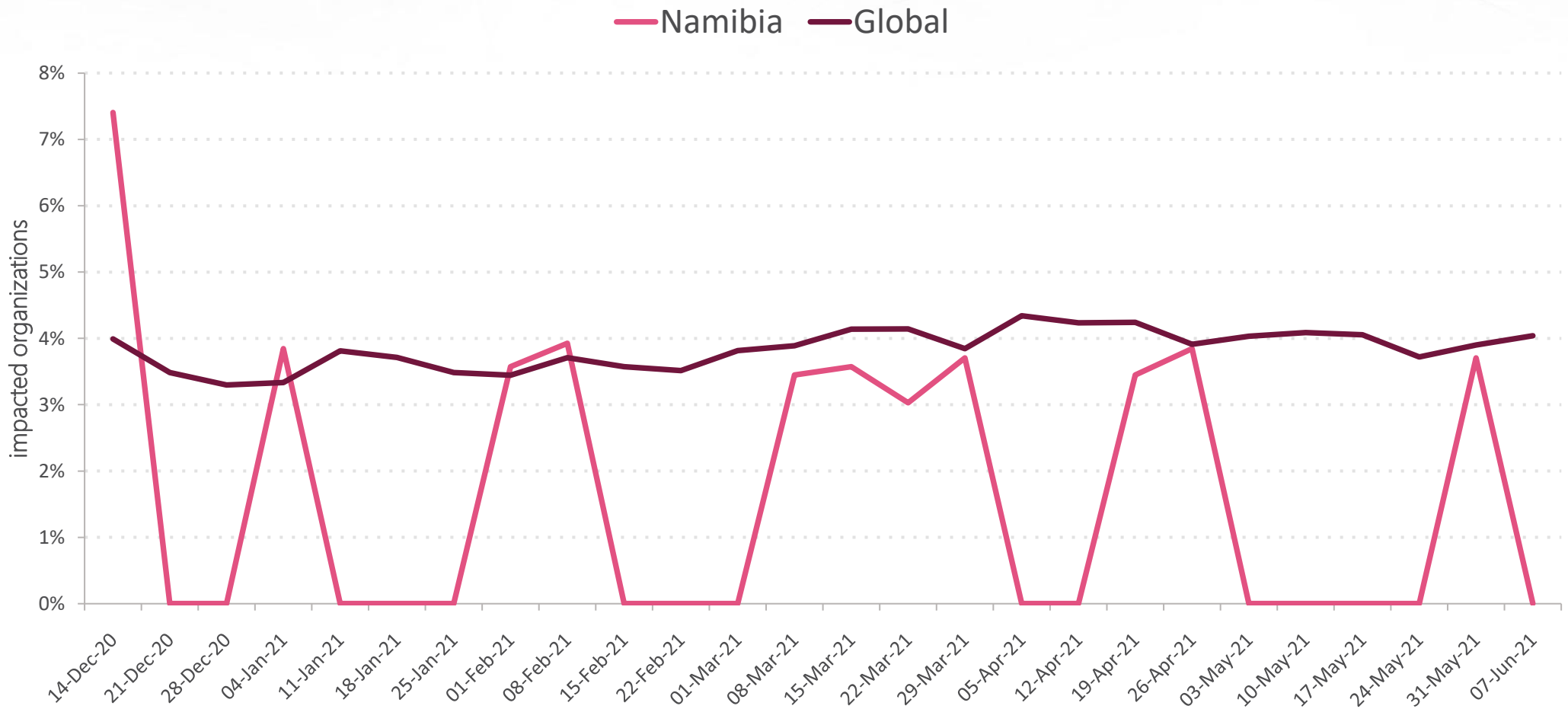
InfoStealer Attacks- Last 6 Months



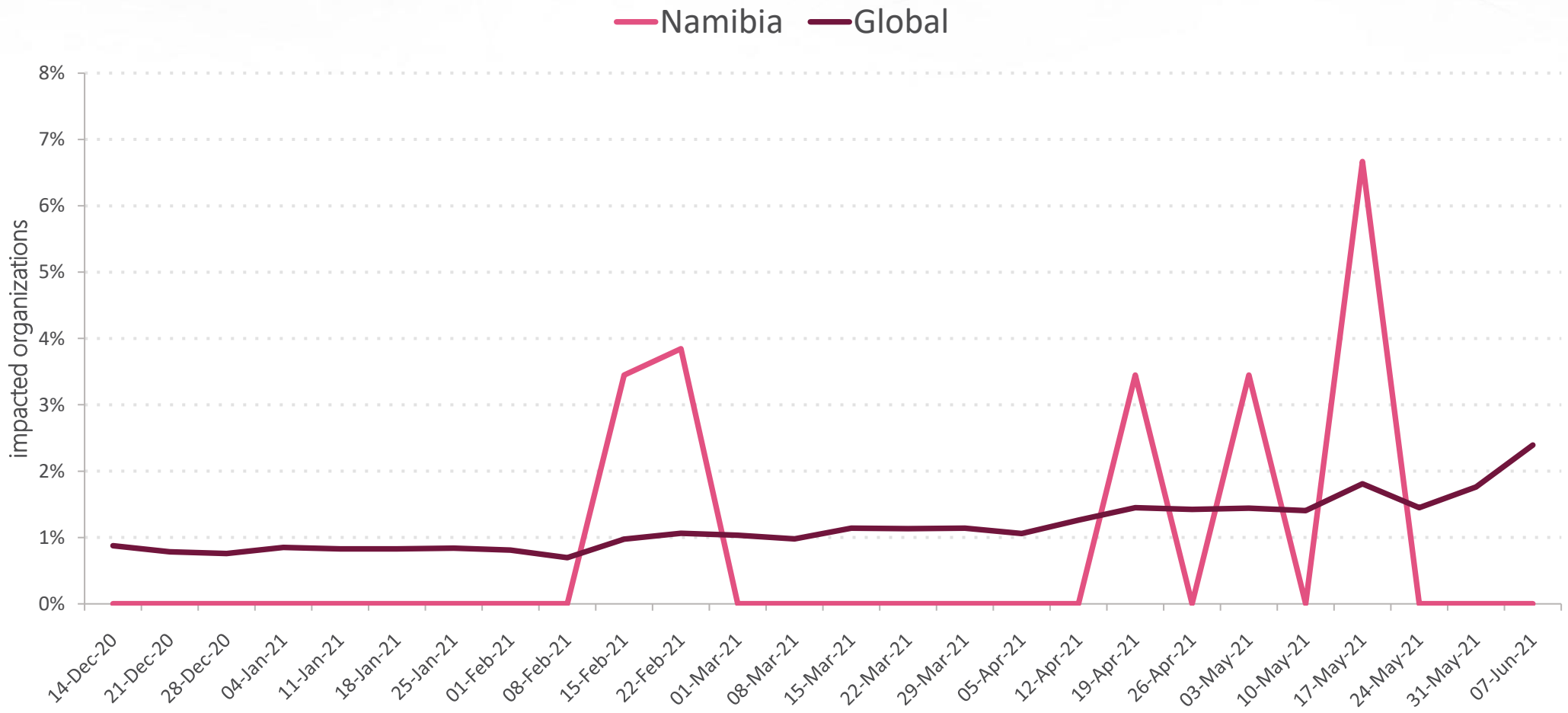
Banking Attacks- Last 6 Months



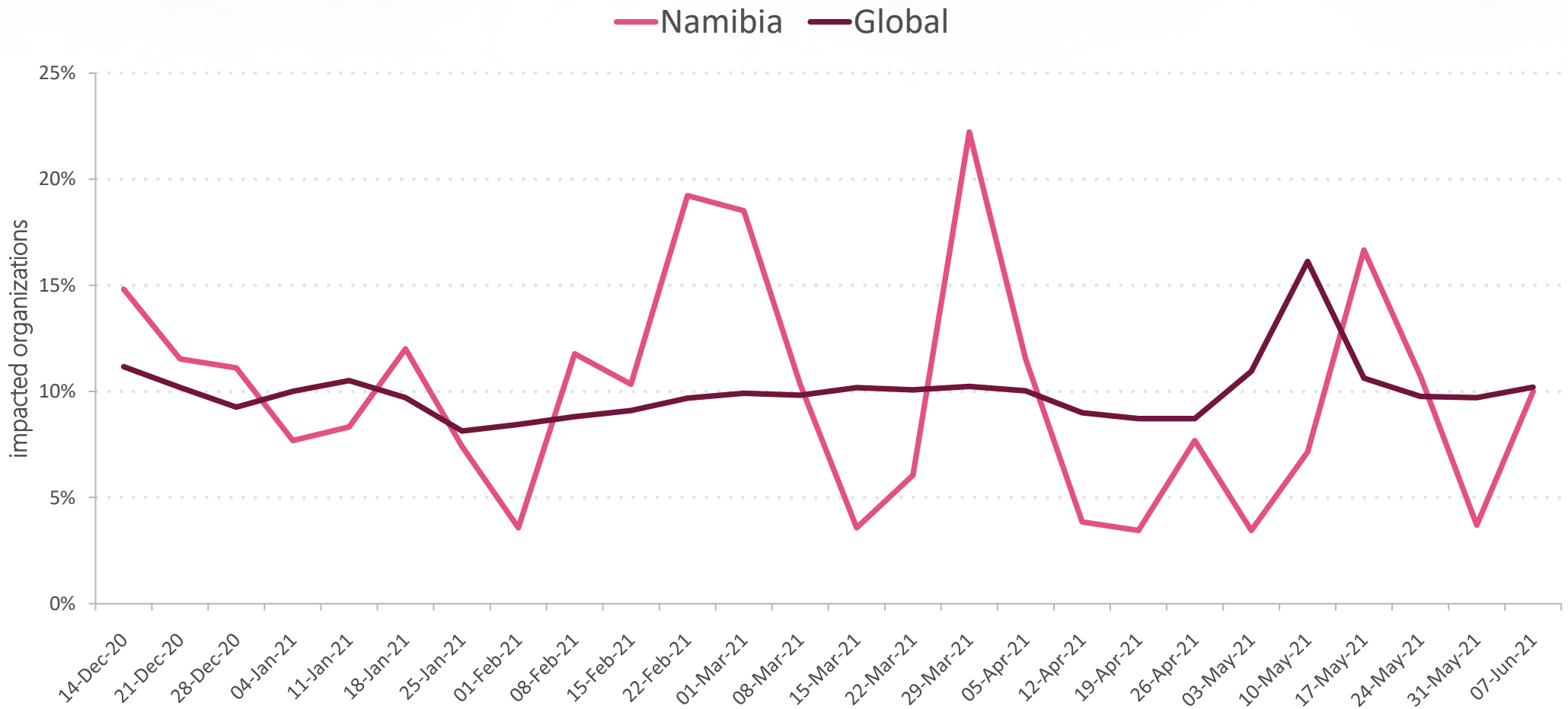
Cryptominer Attacks- Last 6 Months



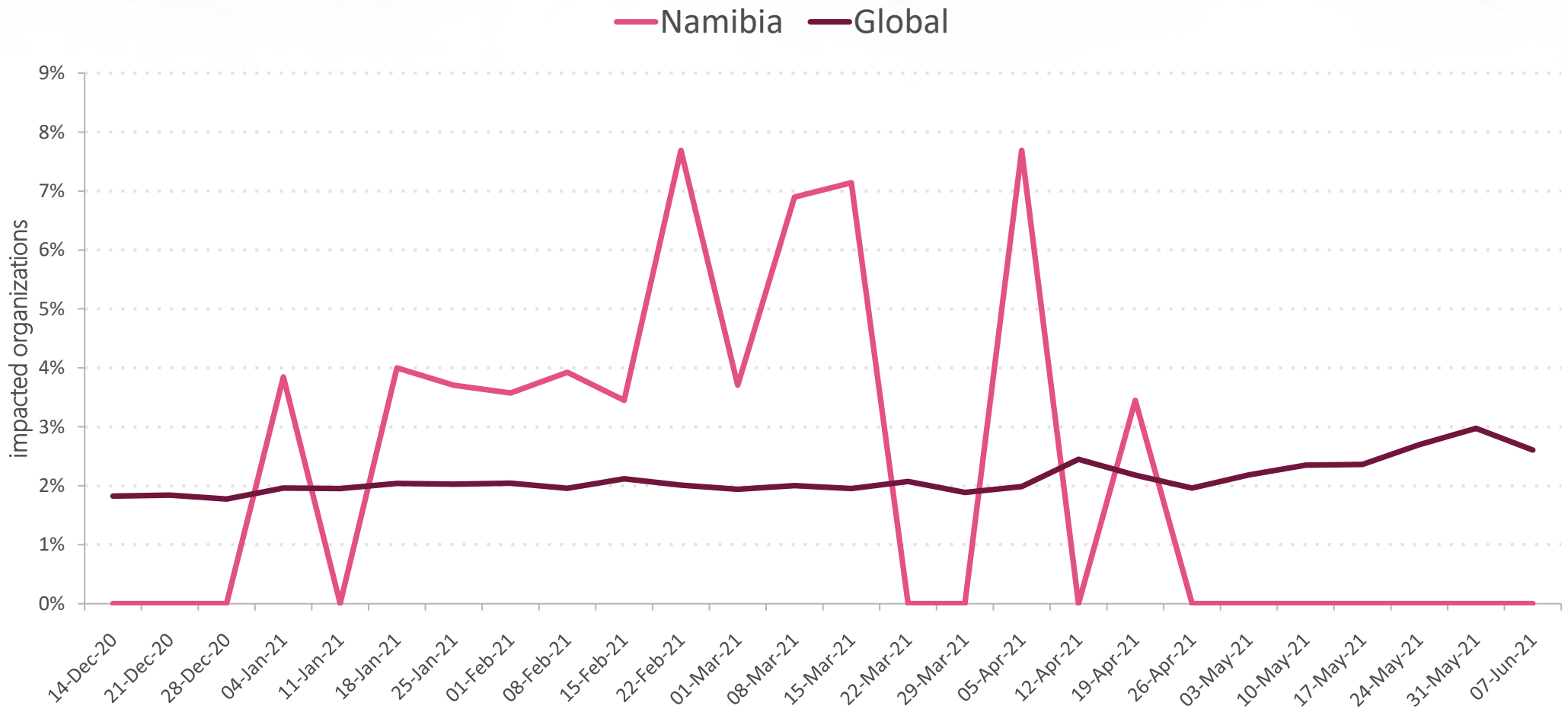
Mobile Attacks- Last 6 Months



Botnet Attacks- Last 6 Months



Ransomware Attacks- Last 6 Months



THANK YOU

More Info:

https://research.checkpoint.com/

cp<r>
CHECK POINT RESEARCH

Check Point
SOFTWARE TECHNOLOGIES LTD