Check Point
SOFTWARE TECHNOLOGIES LTD

cp<r>
CHECK POINT RESEARCH

THREAT INTELLIGENCE-ITALY

WELCOME TO THE FUTURE OF
CYBER SECURITY

POWERED BY CHECK POINT INFINITY

CLOUD • MOBILE • THREAT PREVENTION

Threat Intelligence Summary

- An organization in Italy is being attacked on average 702 times per week in the last 6 months, compared to 606 attacks per organization globally.
- The top malware in Italy is AgentTesla, impacting 7% of organizations.
- The top malware list in Italy includes 2 Cryptominers (Jsecoin, XMRig), 1 Banking Trojan (Trickbot), 1 RAT (AgentTesla) and 1 Infostealer (Hawkeye).
- 88% of the malicious files in Italy were delivered via Email, compared to 35% of malicious files globally.
- The most common vulnerability exploit type in Italy is Information Disclosure, impacting 67% of the organizations.
- Weekly impacted organizations by malware types:

	Mobile	Banking	Cryptominer	Botnet	Ransomware
Italy Avg.	15.0%	6.2%	13.9%	4.7%	1.2%
Global Avg.	20.4%	4.5%	14.5%	7.1%	1.0%

- View the latest publications by Check Point Research

2019H1 Threat Landscape

Check Point
SOFTWARE TECHNOLOGIES LTD

Boutique Ransomware – Ransomware changed their approach and instead of being spread massively, started to preform tailored attacks against organizations, including taking control over their most important assets, and leaving them no other option but paying the ransom reaching to millions of dollars.

Cloud Breaches Lead to Mega Data Breaches – Misconfiguration and poor management of the cloud resources, remain the most prominent threats to the cloud ecosystem - with massive data theft being the most common attack employed against it. The stole data may include: sensitive privet identifiable information, financial data, personal or professional files.

Advance Email Attacks – In 2019 we observed a considerable increase in email scams involving blackmailing such “Sextortion” and “Business Email Compromise” (BEC , which determined to convince victims to pay and don’t necessarily contain malicious links or attachments. The email scammers have also increased the use of evasion techniques in order to bypass email security solutions.

Mobile Evolution- More than 35% of organizations impact by a mobile attack in 2019. Mobile Banking Trojans successfully infiltrated into the mobile arena with a sharp rise of more than 50% in comparison to 2018. Another method highly observed is the increasing utilization of Sandbox Evasion Techniques including using transparent icon with empty application labels and monitoring devices’ motion sensors.

Software Supply Chain attacks – became very prevalent in 2019. In this attack threat actor inserts malware into otherwise legitimate software, by modifying and infecting one of the building blocks this software relies upon. In this way attackers are capable of installing their malware on large distribution radius.

For more data and examples please see Check Point mid-year cyber attack trend report.

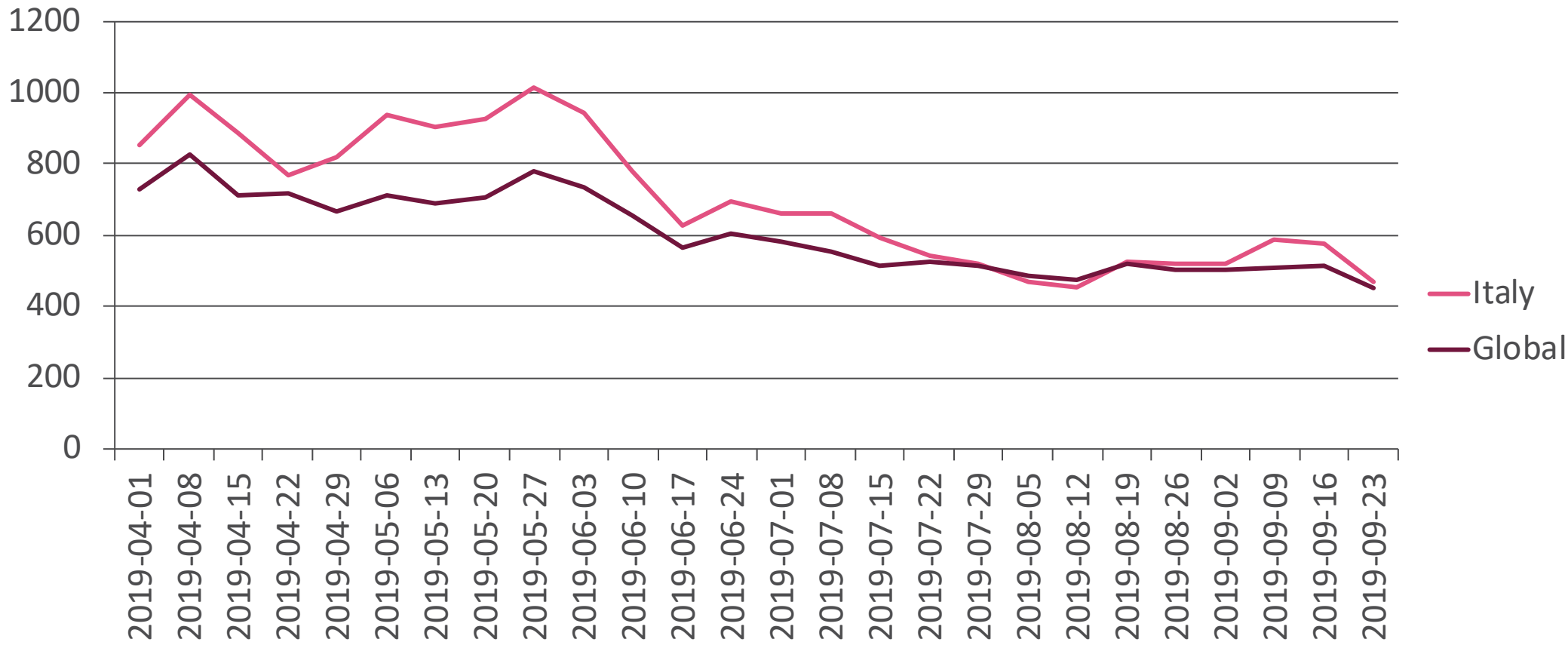
Major attacks and data breaches - Italy

- 08/2019 - A new wave of fraudulent marketing campaigns has been revealed, targeting Italian and Spanish-speaking customers. The campaigns, carried out by a threat group dubbed Lotsy, involve dozens of well-known brands such as Target, Carrefour, Alitalia and more. The group used fake ads for coupons and free gifts containing links to third-party marketing resources and paid services.
- 06/2019 - Months long malspam attack on Italian users deliver variants of Ursnif. A new report details the evolution of the malware.
  - Check Point Anti-Virus and Anti-Bot blades provide protection against this threat (Banking.Win32.Ursnif)
- 05/2019 - The hacking groups LulZSec and Anonymous Italy have been involved in a recent cyber-attack hitting the Italian Ministry of Environment in which they managed to steal data belonging to 30,000 Roman lawyers. The stolen data, which also contained information belonging to the Mayor of Rome, was later published and archived online.
- 04/2019 - Exodus spyware, recently found in Google Play Store directed at Android platforms, has been modified to target Apple iOS mobiles. Deployment of the iOS version was detected outside the App Store through Italian and Turkmenistani phishing sites by abusing Apples Developer Enterprise program.
  - Check Point SandBlast Mobile customers are protected from this threat
- 04/2019 - Researchers have discovered a government Android spyware available on Google Play Store. The spyware, Exodus, disguises as service applications from mobile operators and aimed at Italian users.
  - Check Point SandBlast Mobile customers are protected from this threat

Major attacks and data breaches- Global- 09/2019

- 419 million records of phone number and user IDs of Facebook users have been found on a publicly exposed server that wasnt password protected. The leaked IDs can be used to correlate between the phone numbers and user profiles.
- Attackers have convinced the CEO of an energy company to send $243,000 to a fake supplier using AI to create a deep fake voice impersonation of a chief executive.
- In another recently published ransom attack, the American city of New Bedford Massachusetts has offered to pay $400,000 instead of the requested $5.3 million in exchange for decryption keys. Attackers rejected the proposal and the city resolved to restore its systems from backups.
- Joker, an Android spyware first spotted in June 2019, has been found on 24 different applications on Google Play store. Designed to steal SMS messages, contact lists, device information, the malware targets users from designated 37 countries and has been downloaded by nearly half a million users until removed by Google.
  - Check Point SandBlast Mobile provides protection against this threat
- Nemty, a ransomware previously spotted spreading via compromised Remote Desktop connections, is now using a fake PayPal page and the RIG exploit kit to infect new victims.
  - Check Point IPS, Anti-Virus and Anti-Bot blades provide protection against this threat (RIG Exploit Kit Website Redirection; RIG Exploit Kit Landing Page; Ransomware.Win32.Nemty.TC)

Attacks per Organization - Last 6 Months



Top Malware - Italy- 08-2019

Malware Family	Description	Global Impact	Country Impact
AgentTesla	AgentTesla is an advanced RAT which functions as a keylogger and password stealer and has been active since 2014. AgentTesla can monitor and collect the victim's keyboard input, system clipboard, and can record screenshots and exfiltrate credentials belonging to a variety of software installed on a victim's machine.	5%	7%
Trickbot	A Dyre variant that emerged in October 2016. It targeted bank users mostly in Australia and the UK, and later started focusing on India, Singapore and Malaysia. Trickbot can pull web-injection instructions from its C&C servers online when the victim tries to reach a website. This differs from most banking Trojans that update their configurations periodically, and helps Trickbot avoid mistakes caused by an out-of-date configurations that may lead to its discovery.	5%	5%
Jsecoin	Web-based Crypto miner designed to perform online mining of Monero cryptocurrency when a user visits a particular web page. The implanted JavaScript uses a large amount of the end user machines computational resources to mine coins, thus impacting the system performance.	7%	4%
XMRig	An open source CPU mining software used to mine Monero cryptocurrency. First seen in the wild in May 2017.	7%	4%
Hawkeye	Hawkeye is an Info Stealer malware, designed primarily to steal users' credentials from infected Windows platforms and deliver them to a C&C server. In the past years, Hawkeye has gained the ability to take screenshots, spread via USB and more in addition to its original functions of email and web browser password stealing and keylogging. Hawkeye is often sold as a MaaS (Malware as a Service).	2%	3%

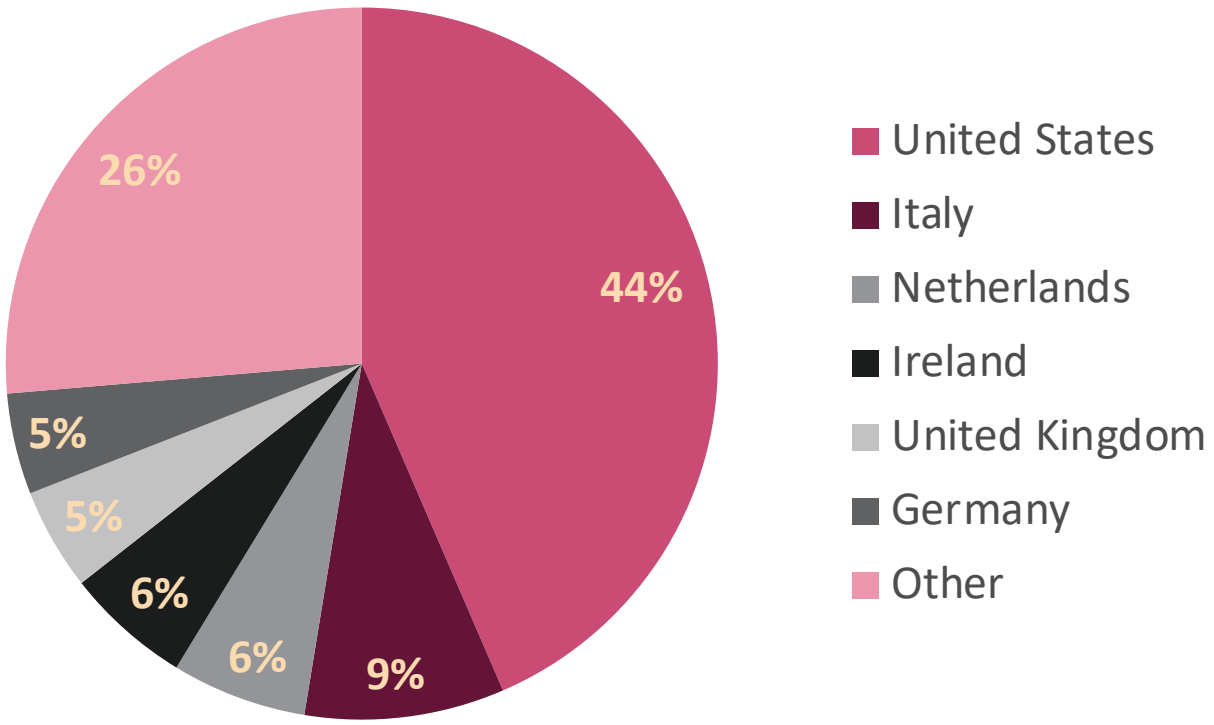
Top Malware - Global- 08-2019

Malware Family	Description	Global Impact
XMRig	An open source CPU mining software used to mine Monero cryptocurrency. First seen in the wild in May 2017.	7%
Jsecoin	Web-based Crypto miner designed to perform online mining of Monero cryptocurrency when a user visits a particular web page. The implanted JavaScript uses a large amount of the end user machines computational resources to mine coins, thus impacting the system performance.	7%
Dorkbot	IRC-based worm designed to allow remote code execution by its operator, and download additional malware to the infected system. The primary goal is to steal sensitive information and launch Denial-of-Service attacks. It installs a user-mode rootkit to prevent viewing or tampering with its files and modifies the registry, ensuring execution each time the system starts. Dorkbot spreads by sending messages with a link to a copy of the worm to the infected user's contacts.	5%
Trickbot	A Dyre variant that emerged in October 2016. It targeted bank users mostly in Australia and the UK, and later started focusing on India, Singapore and Malaysia. Trickbot can pull web-injection instructions from its C&C servers online when the victim tries to reach a website. This differs from most banking Trojans that update their configurations periodically, and helps Trickbot avoid mistakes caused by an out-of-date configurations that may lead to its discovery.	5%
AgentTesla	AgentTesla is an advanced RAT which functions as a keylogger and password stealer and has been active since 2014. AgentTesla can monitor and collect the victim's keyboard input, system clipboard, and can record screenshots and exfiltrate credentials belonging to a variety of software installed on a victim's machine.	5%

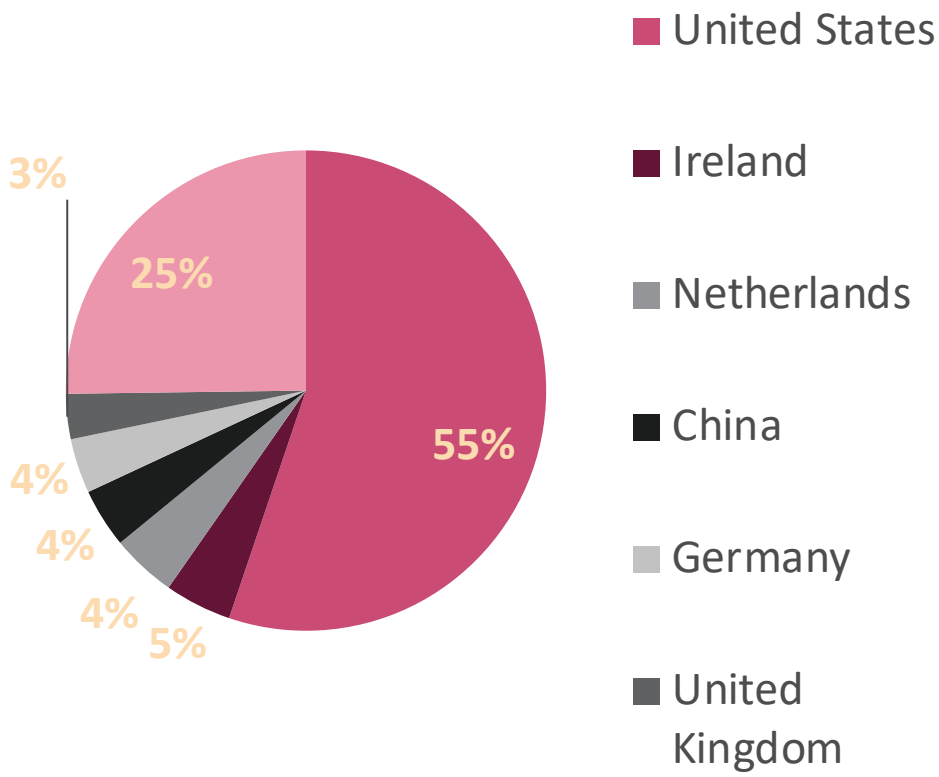
Top Threat Source Countries- Last 6 Months

Check Point
SOFTWARE TECHNOLOGIES LTD

Threat Source Countries- Italy



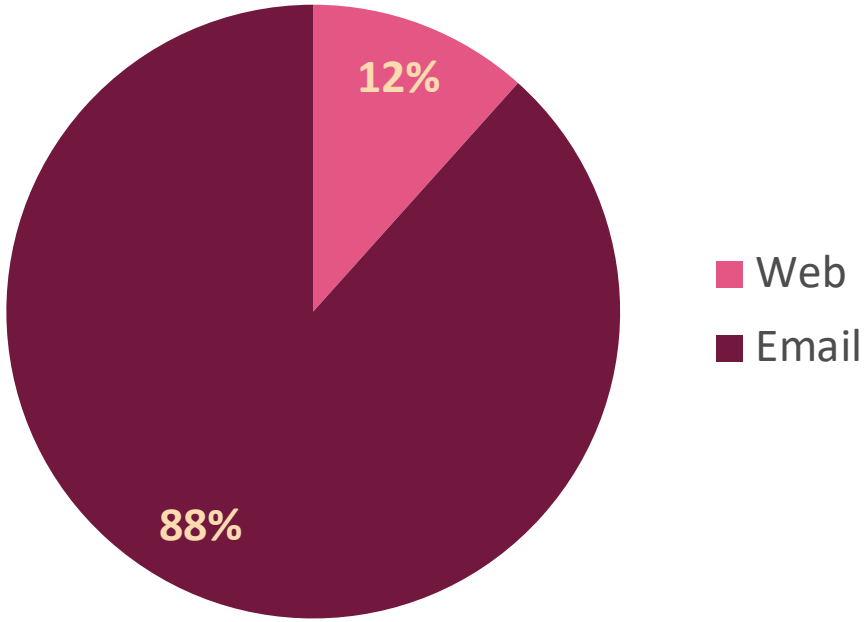
Threat Source Countries- Global



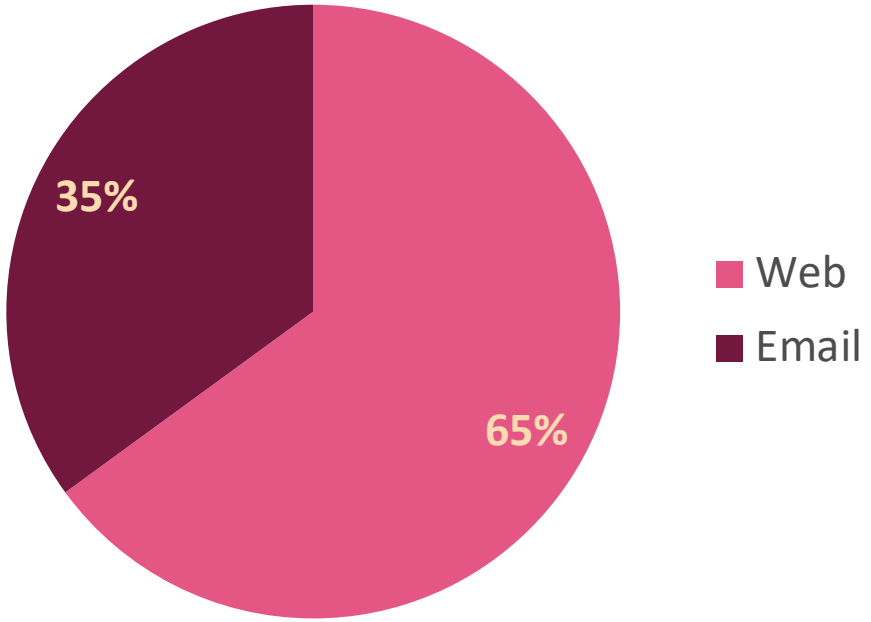
Attack Vector for Malicious Files- Last 3 Months

Check Point
SOFTWARE TECHNOLOGIES LTD

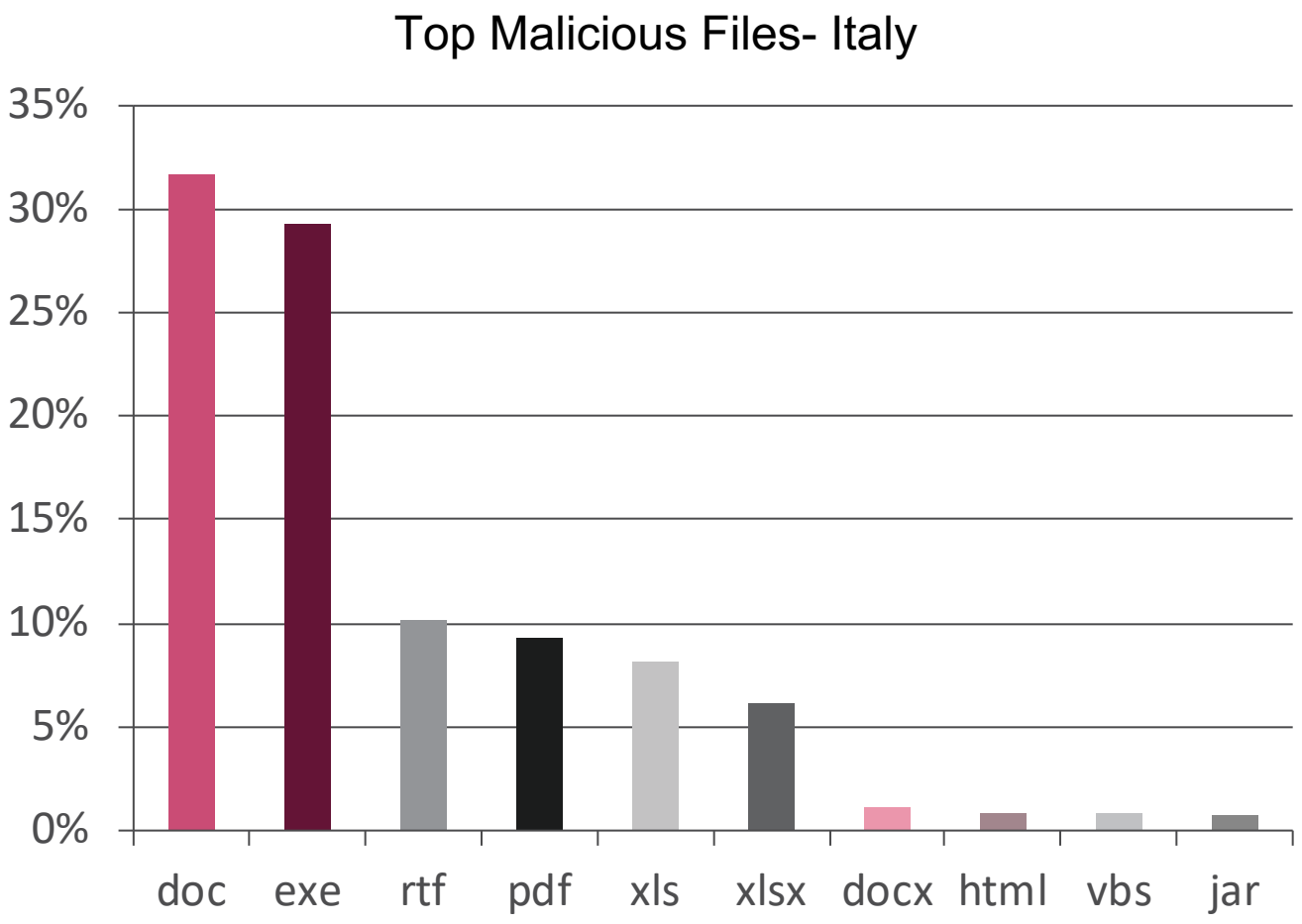
Italy

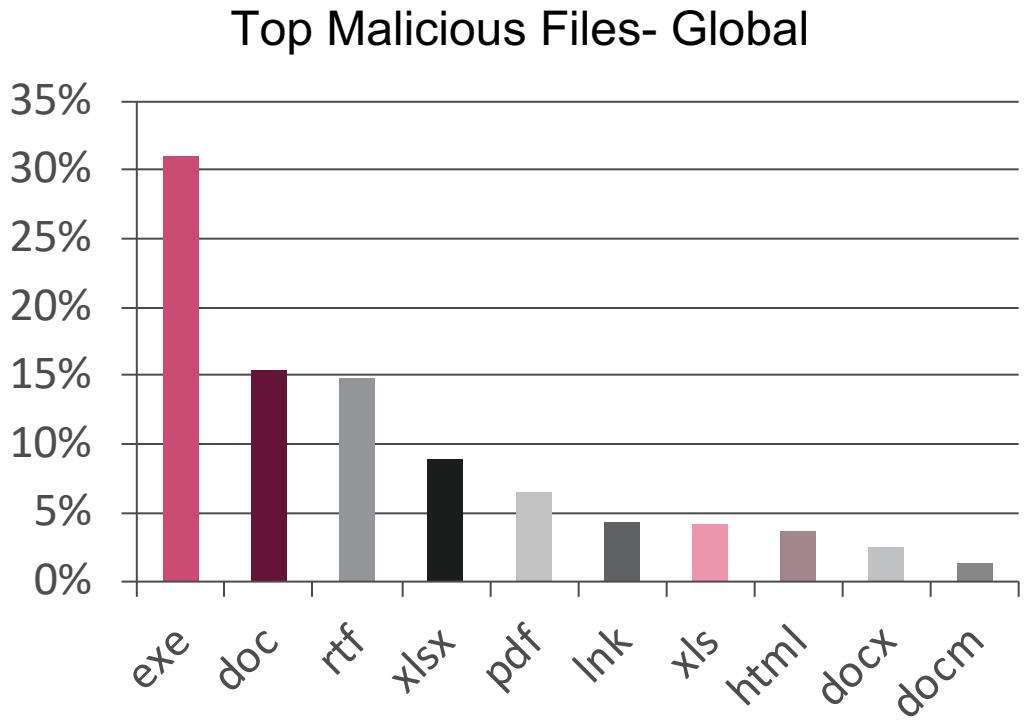


Global

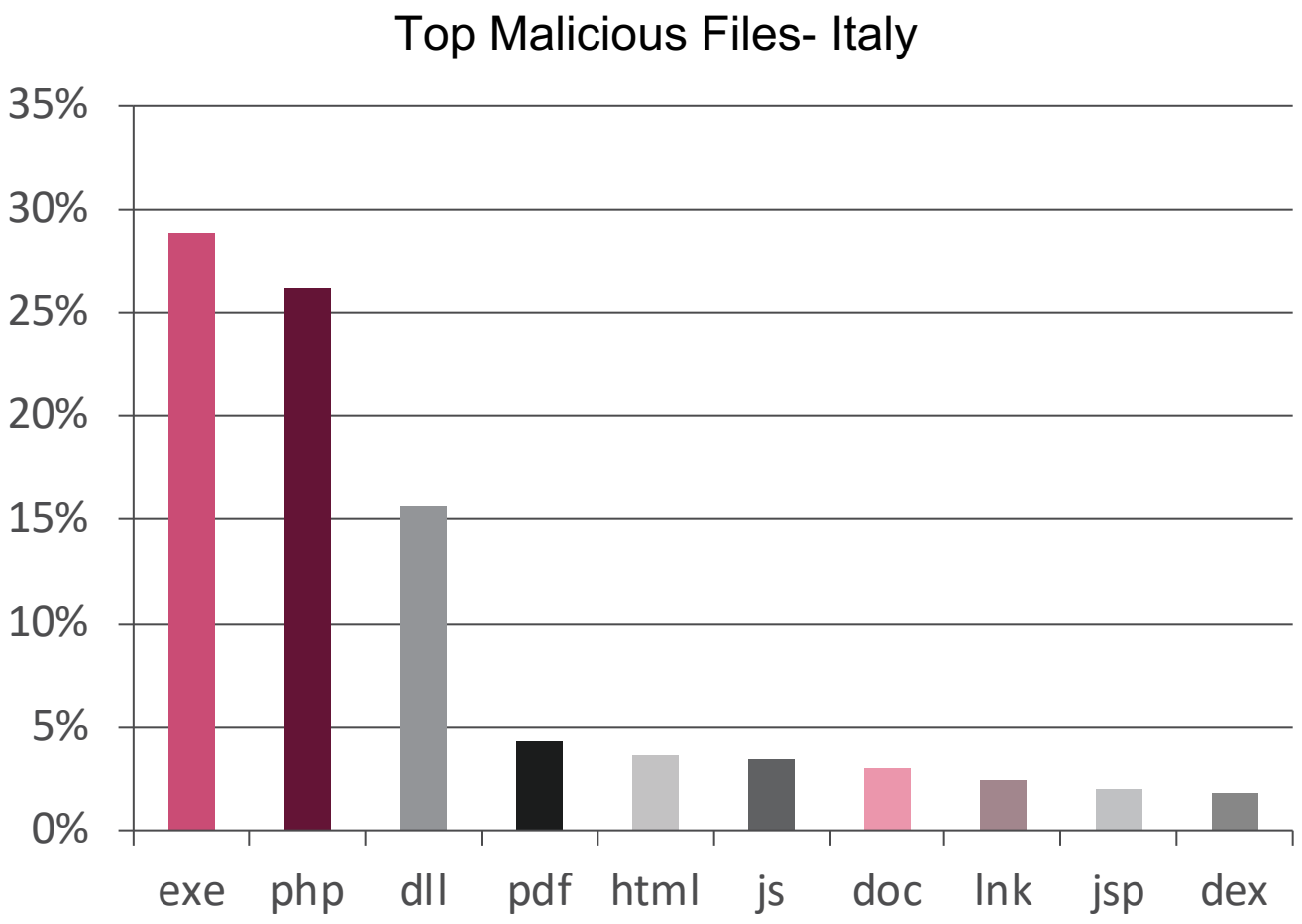


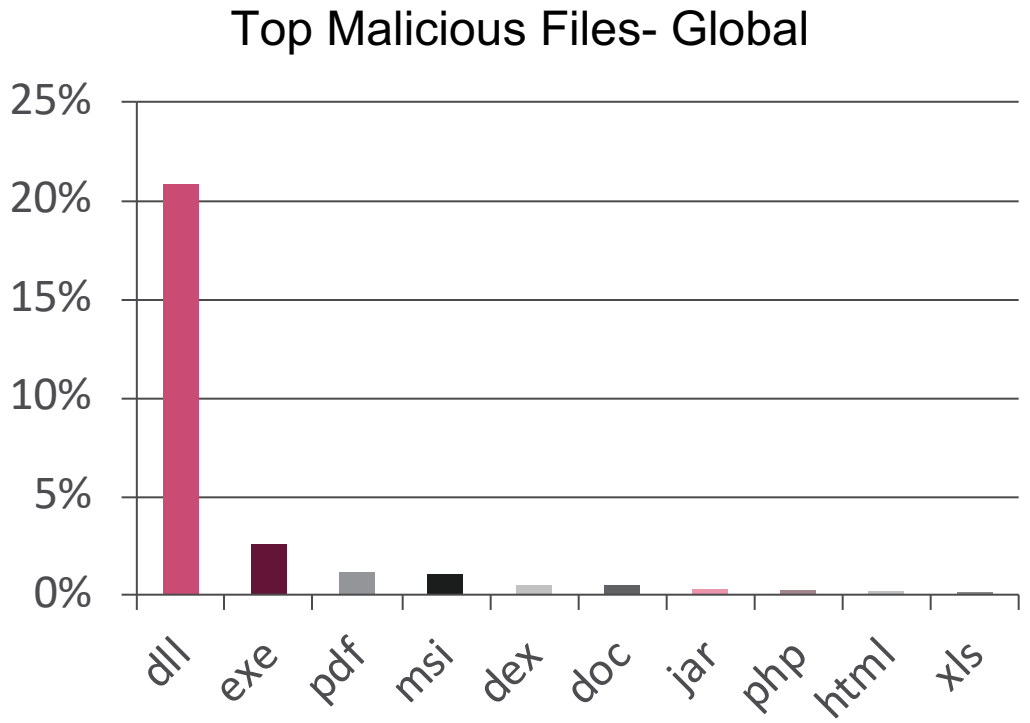
Top Malicious File Types, Email- Last 3 Months



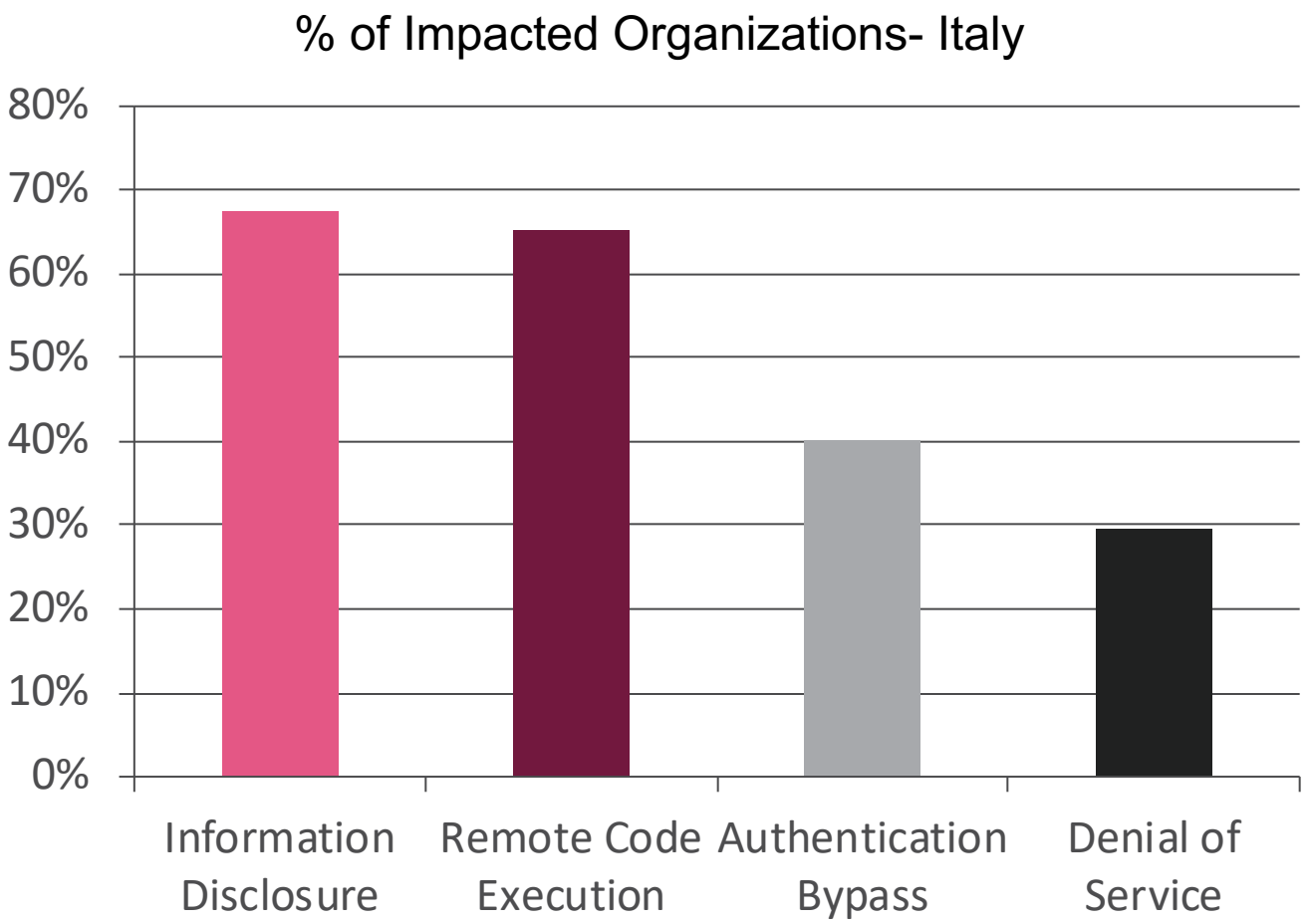


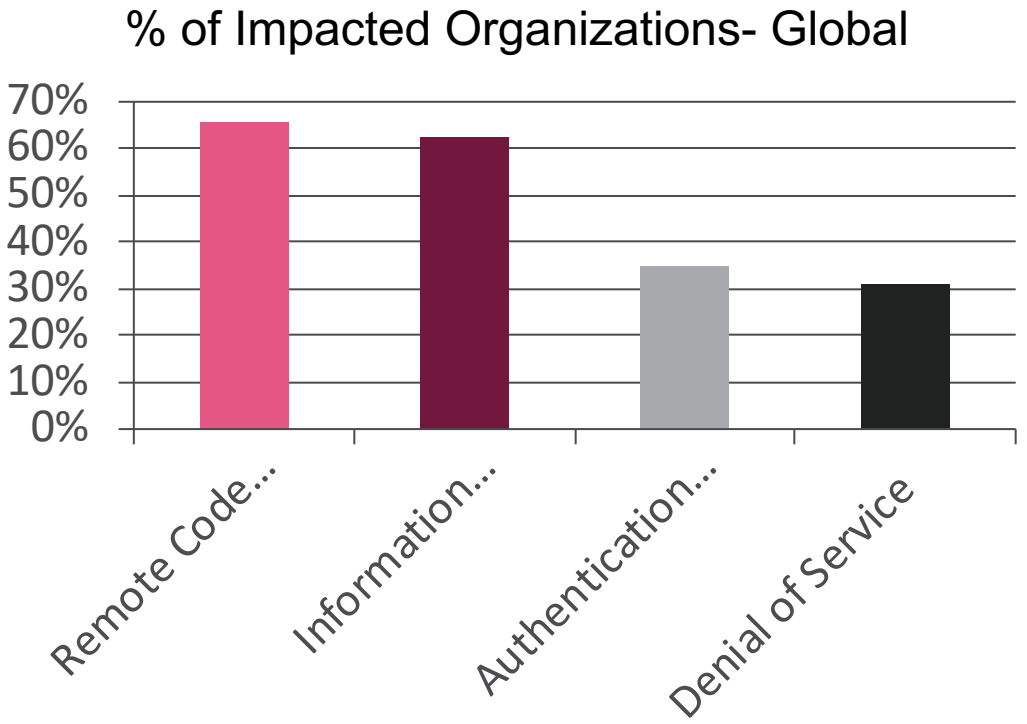
Top Malicious File Types, Web- Last 3 Months



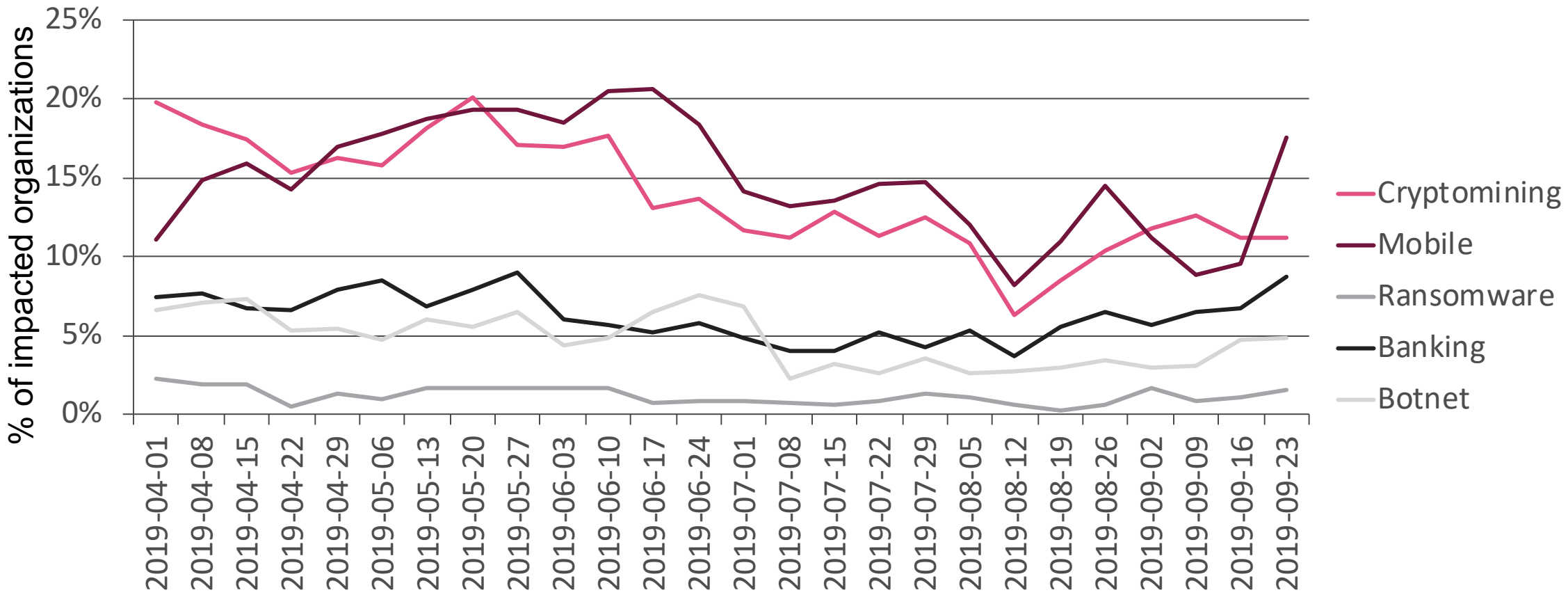


Top Vulnerability Exploit types - Last 30 Days

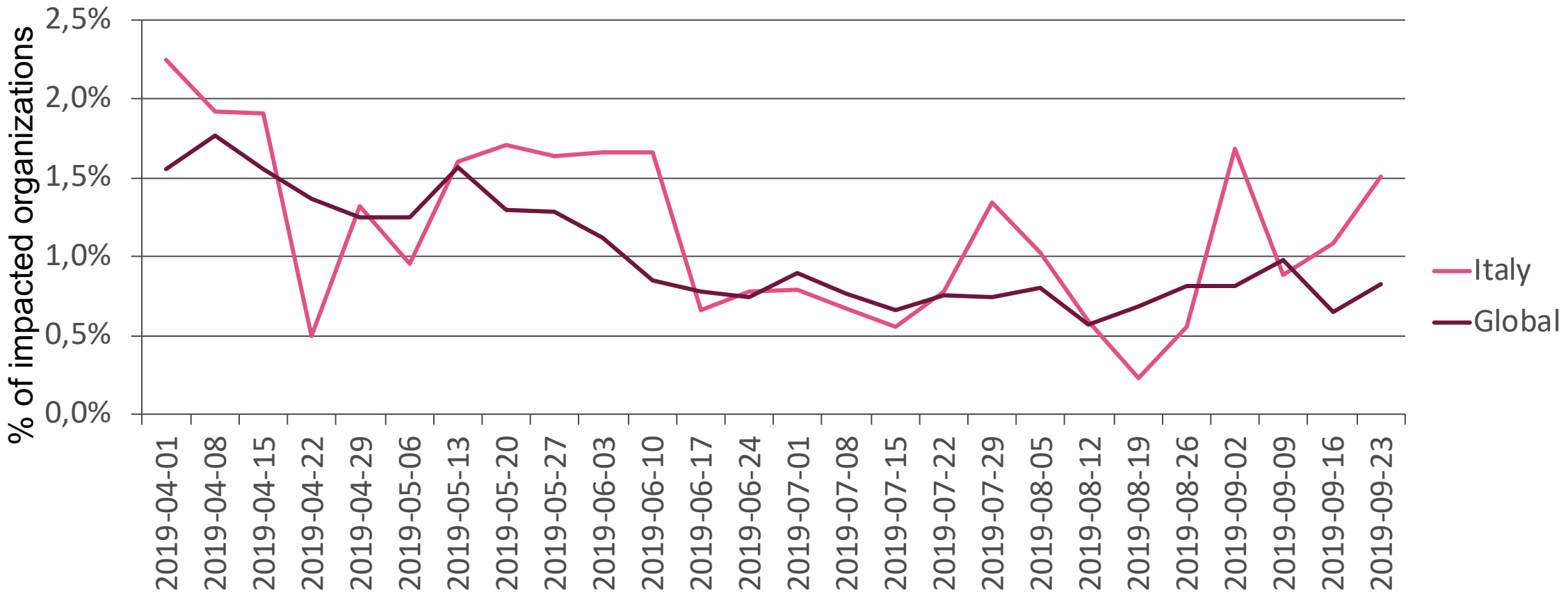




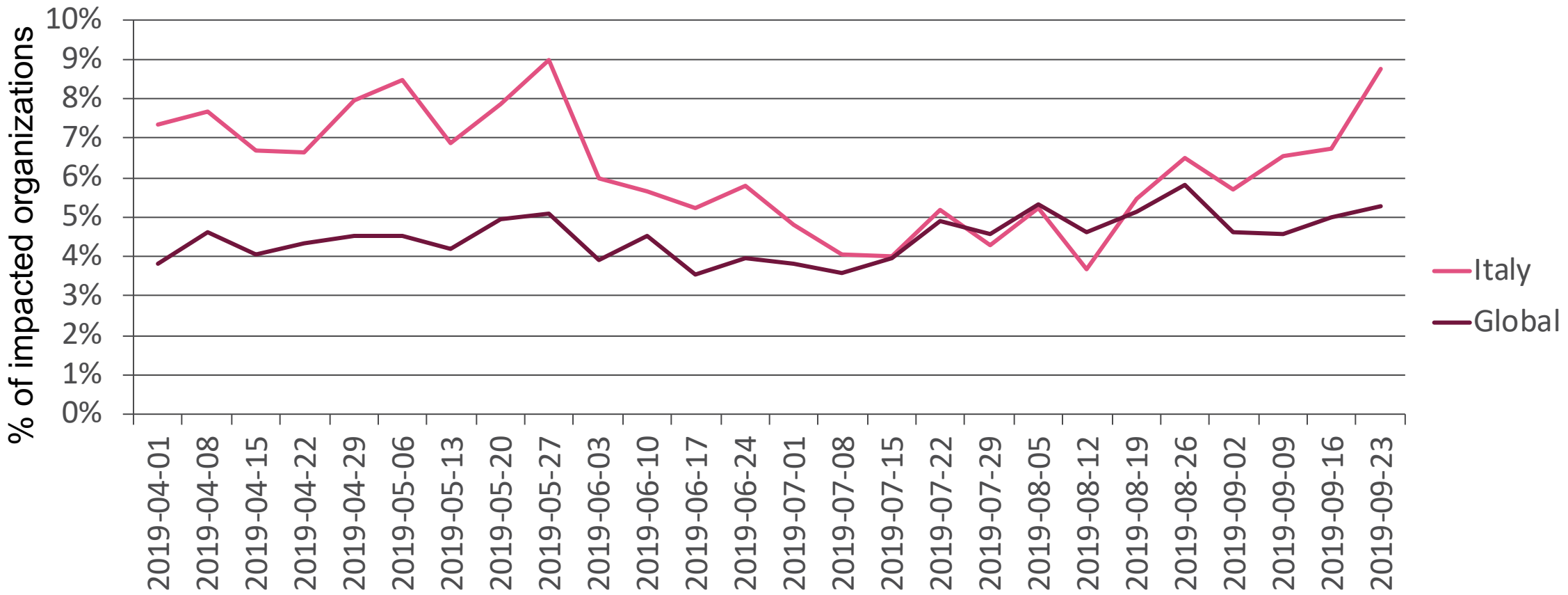
Major Malware Types trend - Last 6 Months



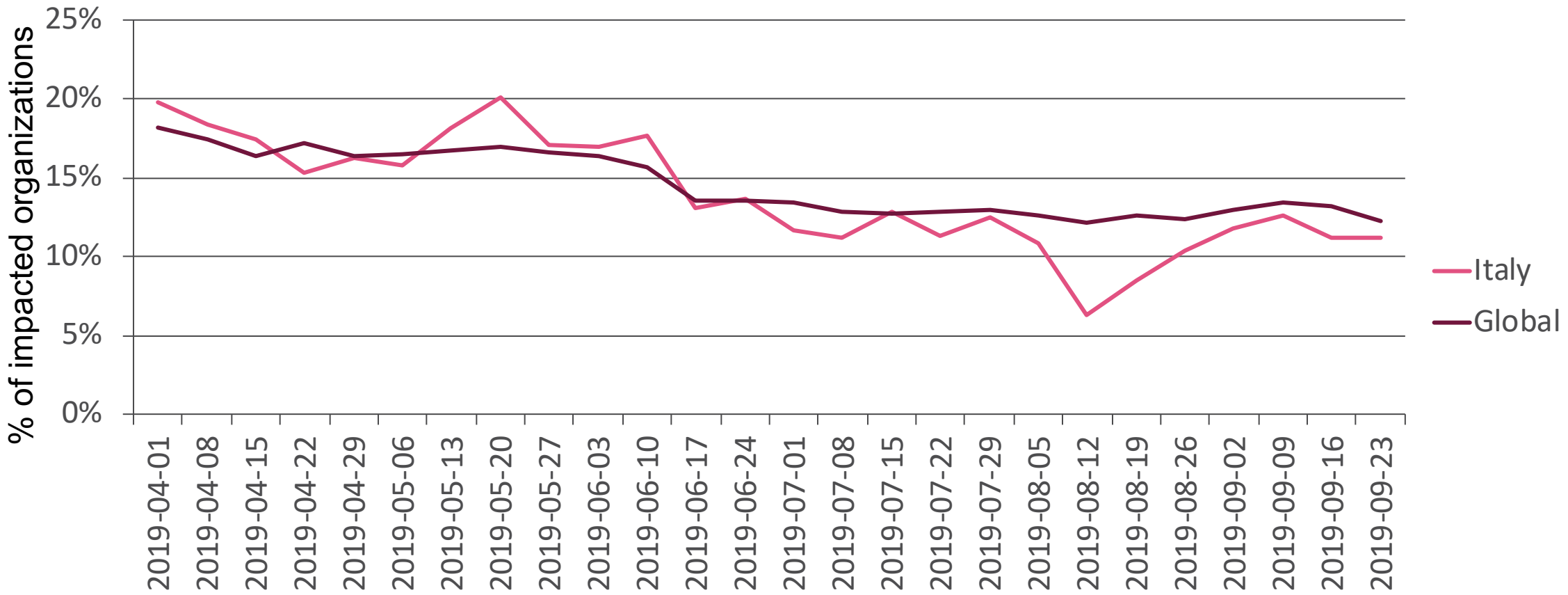
Ransomware Attacks- Last 6 Months



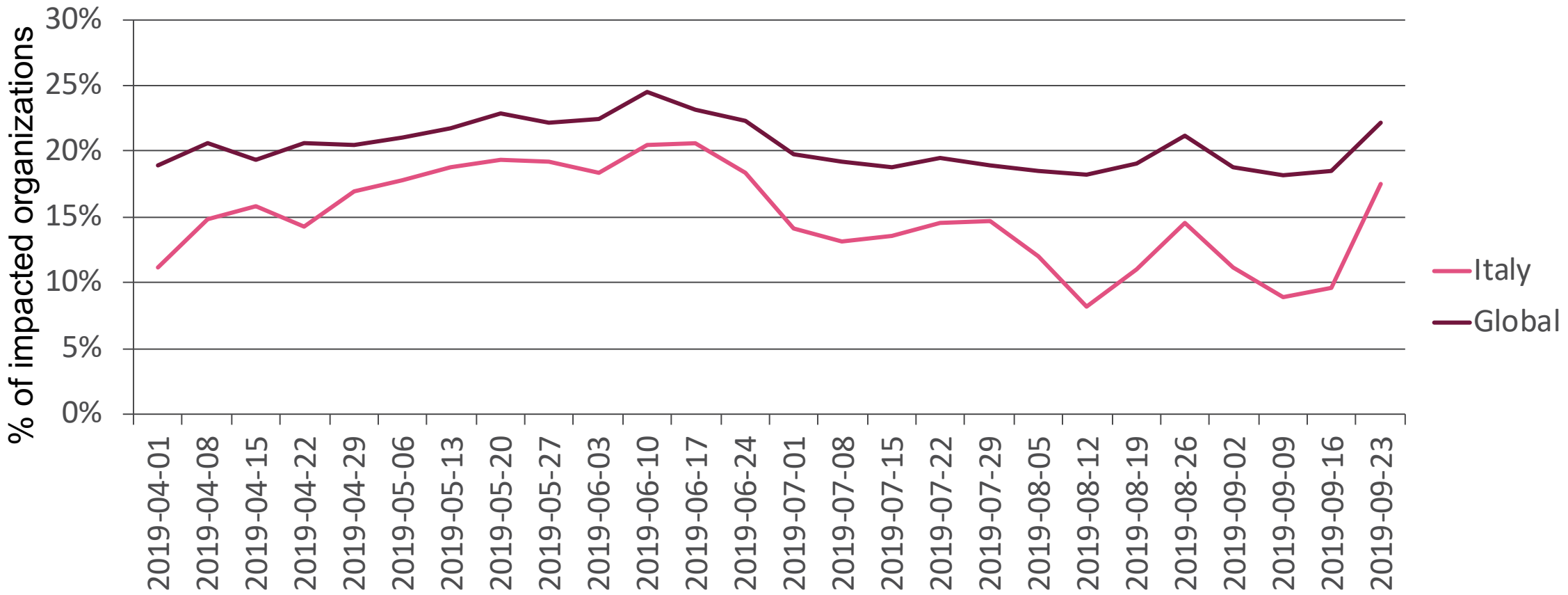
Banking Attacks- Last 6 Months



Cryptomining Attacks- Last 6 Months



Mobile Attacks- Last 6 Months



Botnet Attacks- Last 6 Months

Check Point
SOFTWARE TECHNOLOGIES LTD

cp<r>
CHECK POINT RESEARCH

THANK YOU

More Info:
https://research.checkpoint.com/

WELCOME TO THE FUTURE OF
CYBER SECURITY
POWERED BY CHECK POINT INFINITY

CLOUD • MOBILE • THREAT PREVENTION