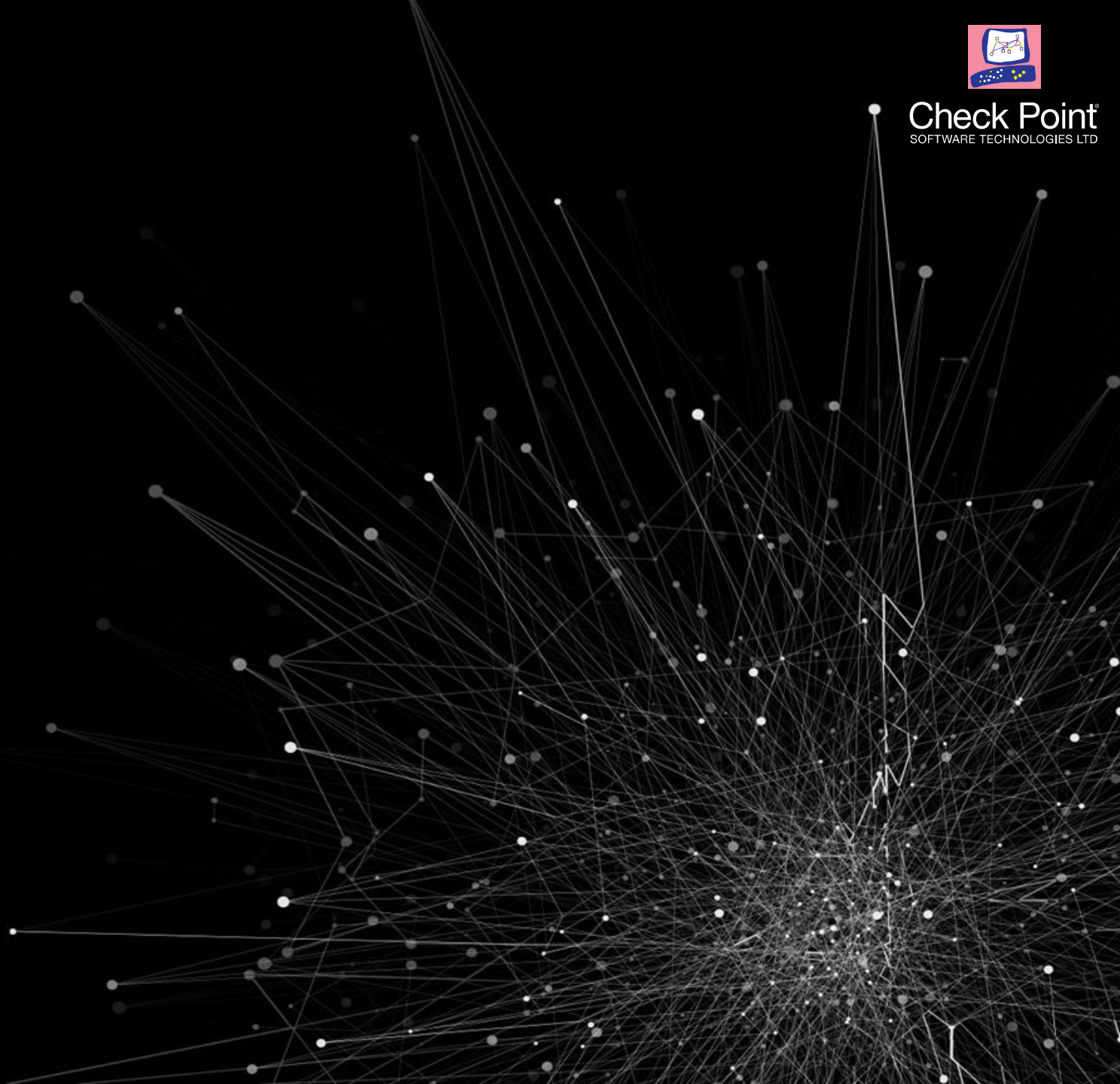
Check Point
SOFTWARE TECHNOLOGIES LTD

THREAT INTELLIGENCE REPORT

Poland

cp<r>
CHECK POINT RESEARCH



Threat Intelligence Summary

- An organization in Poland is being attacked on average 322 times per week in the last 6 months.
- The top malware in Poland is Emotet, impacting 8% of organizations.
- The top malware list in Poland includes 2 Banking Trojans (Trickbot, Ursnif), 1 Spyware (Agenttesla) and 1 Botnet (Emotet).
- 67% of the malicious files in Poland were delivered via Email.
- The most common vulnerability exploit type in Poland is Remote Code Execution, impacting 64% of the organizations.
- Weekly impacted organizations by malware types:

	Mobile	Banking	Cryptominer	Botnet	InfoStealer
Poland Avg.	1.4%	2.9%	3.0%	8.5%	2.5%
Global Avg.	3.6%	2.6%	5.1%	7.1%	2.6%

- View the latest publications by Check Point Research

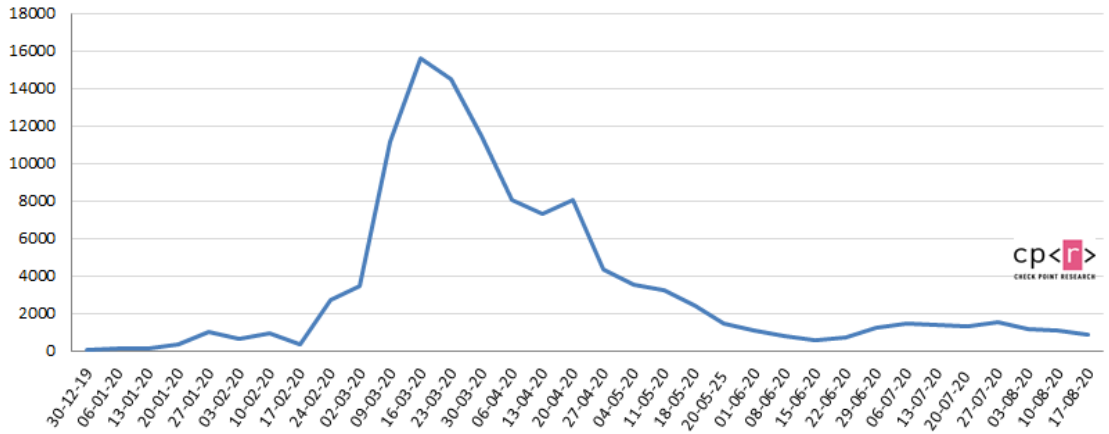
Threat Landscape

- **Double Extortion -** Ransomware actors have adopted a new strategy; in addition to making the victim's files inaccessible, they now exfiltrate large quantities of data prior to its encryption in the final stage of the attack. Victims who refuse payment demands find their most sensitive data publicly displayed on dedicated websites.
- **Cyber Warfare -** Nation-state cyber activity has seen a surge in intensity and escalation in severity. In times when traditional tactics to gather intelligence and knowledge are no longer feasible due to social distancing, the use of offensive cyber weapons to support national missions appears to have expanded. The goal may be better understanding of the Corona virus or securing intelligence operations, and countries and industries are the targets.
- **Mobile -** Threat actors have been seeking new infection vectors in the mobile world, changing and improving their techniques to avoid detection in places such as the official application stores. In one innovative attack, threat actors used a large international corporation's Mobile Device Management (MDM) system to distribute malware to more than 75% of its managed mobile devices.
- **Cloud -** Industries were required to make rapid infrastructure adjustments to secure their production when working remotely. In many cases, this would not have been possible without cloud technologies. However, it also exposed more misconfigured or simply unprotected assets to the internet. In addition, for the first time, alarming vulnerabilities were revealed in Microsoft Azure infrastructure that could enable invaders to escape VM infrastructure and compromise other customers.
- **Pandemic Cyber Landscape -** COVID-19 affected every aspect of our life, cyber landscape included. From an upsurge of registration of Corona related domains to use of related topics in phishing attacks. Medical services and research organizations became targets to attacks seeking ransom or valuable commercial and professional information. Use of tracking systems, which previously would have caused extreme privacy related opposition, became prevalent around the world and in some cases is expected to outlive the emergency.
- For more data and examples please see Check Point Research Cyber Attack Trends: 2020 Mid-Year Report.

Coronavirus - Cyber Updates

- Since the Coronavirus pandemic outbreak we have witnessed a rise in registration of new Corona related domains, many of those may be used for malicious activity.

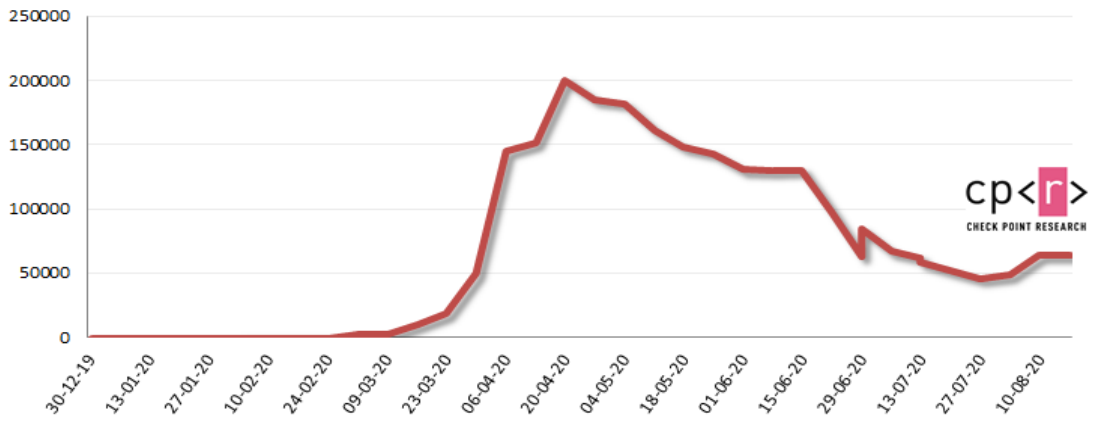
Coronavirus Domains Registered Weekly



- Cyber criminals are also targeting other aspects of the new life routine, targeting and imitating video conference applications, media streaming services, Stimulus and relief packages payment transfer, money loans, Job application.

- The global interest in the Coronavirus leads cyber criminals to use Corona related themes in order to lure victims to download malicious applications and files or clicking on malicious links.

Weekly Coronavirus Related Cyber Attacks



- The attacks are taking place in many platforms and include malicious corona related apps, websites related to corona, and targeted emails using the corona pandemic at their email subject/file names.

Coronavirus - Cyber Updates

- Voice phishing attacks are on the rise due to COVID-19 remote work policies and following the high-profile Twitter vishing scam. Researchers describe coordinated attacks, leasing of American voice actors, set-up of dedicated phishing pages to bypass MFA mechanism, in campaigns often focusing on corporate new hires.
- Thousands of Canadian government services accounts have been hacked in credentials stuffing attacks, some were later used to divert COVID-19 aid payments.
- Advisories from the UK, US, Canada and Australia warn that Russia's Foreign Intelligence Service (SVR) has been conducting espionage operations to target COVID-19 research organizations. APT29 (aka Cozy Bear) is believed to be behind the operation, using the WellMess malware.
- Check Point Research has analyzed the latest Coronavirus-themed cyber-attacks. As businesses transition their workforces back to the office, hackers are distributing phishing emails and malicious files disguised as Coronavirus training materials. The latest data also shows that the risk of an organization being impacted by a malicious coronavirus-related website depends on whether the country it is located in has gone back to business or is still under lockdown.
- Check Point researchers have addressed the possible security and privacy risks users of the COVID-19 contact-tracing applications face, from GPS tracking and data collection to fake applications and unauthorized data theft.
  - Check Point SandBlast Mobile provides protection against this threat
- New ransomware called FuckUnicorn has been targeting Italian health entities through emails with links to a COVID-19-related app for PC. The links direct users to a malicious domain imitating the site of the Italian Pharmacist Federation. Researchers suspect the actors behind this attack are Italians.
  - Check Point Anti-Virus product provides protection against this threat (backdoor.Win32.qnode)
- APT36, Pakistani state-sponsored threat actor, has been spreading the Crimson RAT via a spear-phishing campaign using coronavirus themed document disguised to a health advisory email. The RAT steals credentials from the victims browser, captures screenshots, collects anti-virus software information, lists running processes, and more.
- Check Point Research has discovered 16 malicious apps, all masquerading as legitimate coronavirus-related apps, which contained a range of malware aimed at stealing users' sensitive information or generating fraudulent revenues from premium-rate services.
  - Check Point SandBlast Mobile provides protection against this threat.

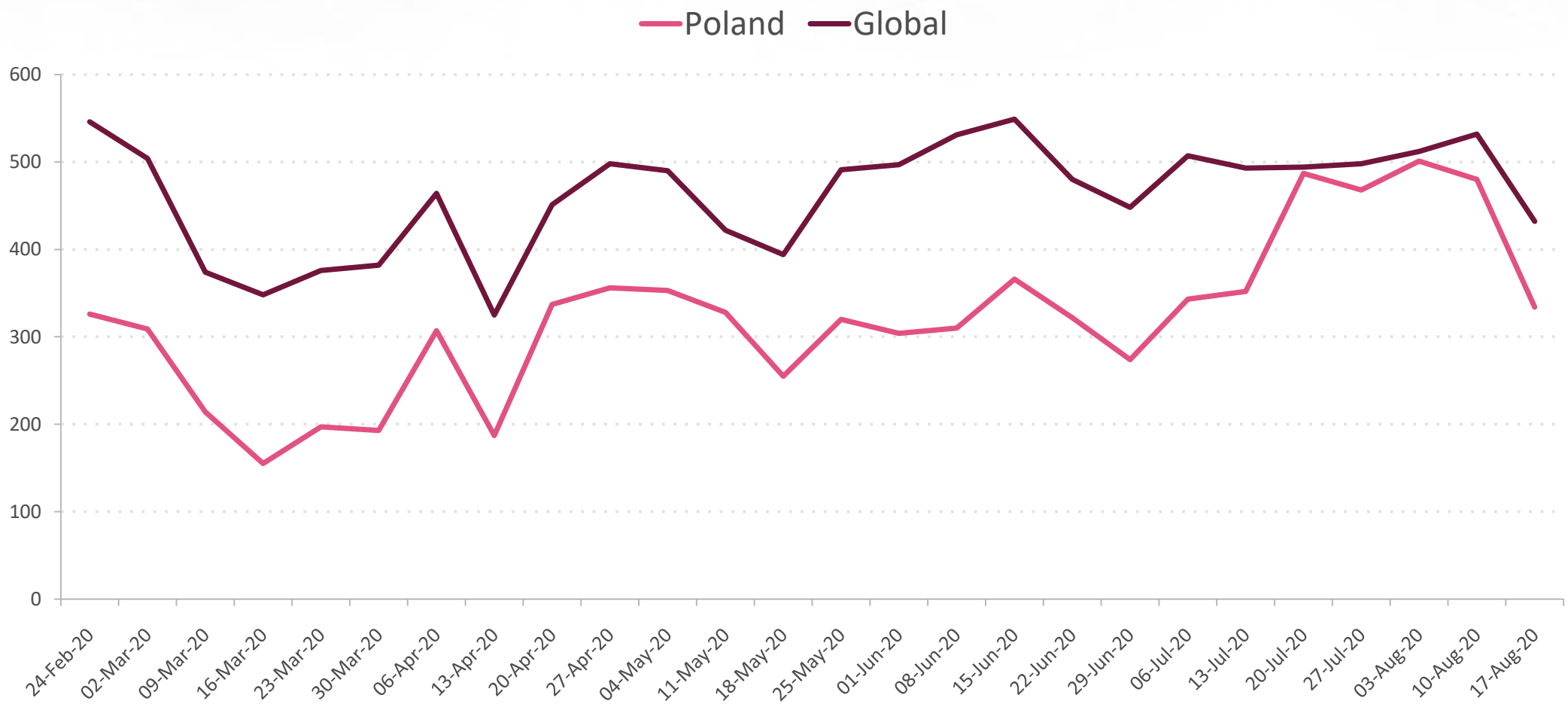
Major attacks and data breaches - Poland

- Aug-20 - An anti-NATO disinformation campaign has been using compromised news websites in Poland and Lithuania to plant false stories aimed to discredit NATO.
- Jan-20 - Researchers report TrickBot operators have developed and used a new PowerShell backdoor for high value targets named PowerTrick. Trickbot has been developed continuously since its initial detection in 2016 and PowerTrick is designed to enhance its ability to bypass restrictions and security controls.
  - New report follows the continuing operations of the North Korean Lazarus APT group targeting cryptocurrency related websites. New findings show the sequel of the 2018 AppleJeus operation using advanced TTPs with new victims in the UK, Poland, Russia and China.
- Jan-19 - APT28 Russian group, has spottedf uses spear-phishing emails on political organizations in Belgium, France, Germany, Poland, Romania, and Serbia in order to collect login credentials or infect them with malware.
  - Check SandBlast, Anti-Bot and Point Anti-Virus blades provide protection against this threat (Trojan-PSW.Win32.Sofacy; Backdoor.Win32.Zebrocy)
- Oct-18 - New APT group has been spotted dubbed GreyEnergy and considered a successor to the infamous BlackEnergy APT group. GreyEnergy uses its own malware framework to conduct cyber espionage operations in Ukraine and Poland, focusing mainly on critical infrastructures. Some of the malwares modules are backdoor, file extraction, taking screenshots, keylogging, password and credential stealing.
  - Check Point Anti-Bot and Anti-Virus blades provide protection against this threat (Trojan.Win32.GreyEnergy)
- Oct-18 - Three energy and transport companies in Poland and Ukraine were suffered from a cyber attack probably by hacker group that has a connection to the Russian intelligence agency, GRU. The hackers used a malware named "GreyEnergy" that allowed them to map out the networks and gather confidential information such as passwords and login credentials
  - Check Point Anti-Bot and Anti-Virus blades provide protection against this threat (Trojan.Win32.GreyEnergy)
- Sep-18 - DanaBot banking trojan in now expanding its targets and is being distributed to European countries such as Austria, Germany, Italy, Poland, and Ukraine. Users in those countries are getting spam emails with a malicious document containing the malware.
  - Check Point SandBlast and Anti-Bot blades provide protection against this threat (Trojan-banker.Win32.Danabot)

Major attacks and data breaches- Global- Last Month

- Data of more than 200K users of Utah-based gun exchange sites has been leaked, and is offered free of charge on a cybercrime forum. According to researchers, the three leaked guns-related databases were all hosted on the same Amazon cloud server.
- Maze ransomware-gang has published a 2.2GB archive comprising of files allegedly stolen from Canon during a ransomware attack earlier this month.
  - Check Point SandBlast Anti-Ransomware and Anti-Bot provide protection against this (Ransomware.Win32.Maze)
- Sodinokibi ransomware group has compromised Jack Daniels whiskey manufacturer the Brown-Forman spirits group. The threat actor claimed they spent a month inside Brown-Formans systems and exfiltrated 1 TB of corporate data, but according to the company it stopped the attack before data was encrypted.
  - Check Point SandBlast Anti-Ransomware provides protection against this threat
- The Israeli Defense Ministry has accused the North Korean related Lazarus APT group in targeting employees of major Israeli defense companies through fake LinkedIn profiles. Researchers said that unlike the groups regular financially motivated attacks, the current campaign was focused on technology theft.
- The SANS information security training institute has suffered a data breach comprised of 27,000 records of PII (Personally Identifiable Information) which were forwarded to an external email address. SANS traced the source of the attack to a phishing email.
- The city of Lafayette Colorado has fallen victim to a ransomware attack and paid the criminals ransom demand of $45,000. The attack was not part of a targeted campaign and the undisclosed ransomware entered the citys systems through phishing or brute force attack.

Attacks per Organization - Last 6 Months



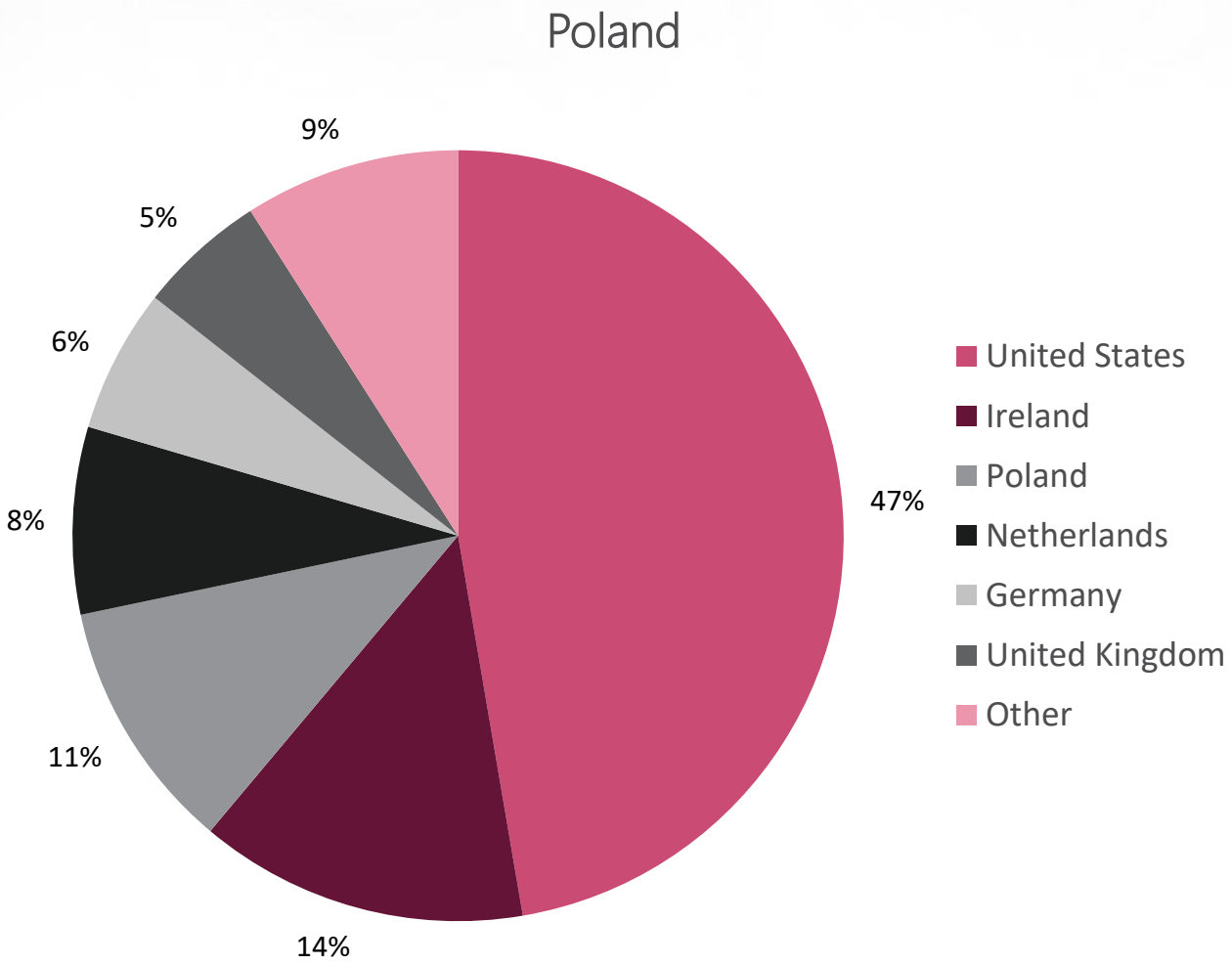
Top Malware - Poland- Jul-20

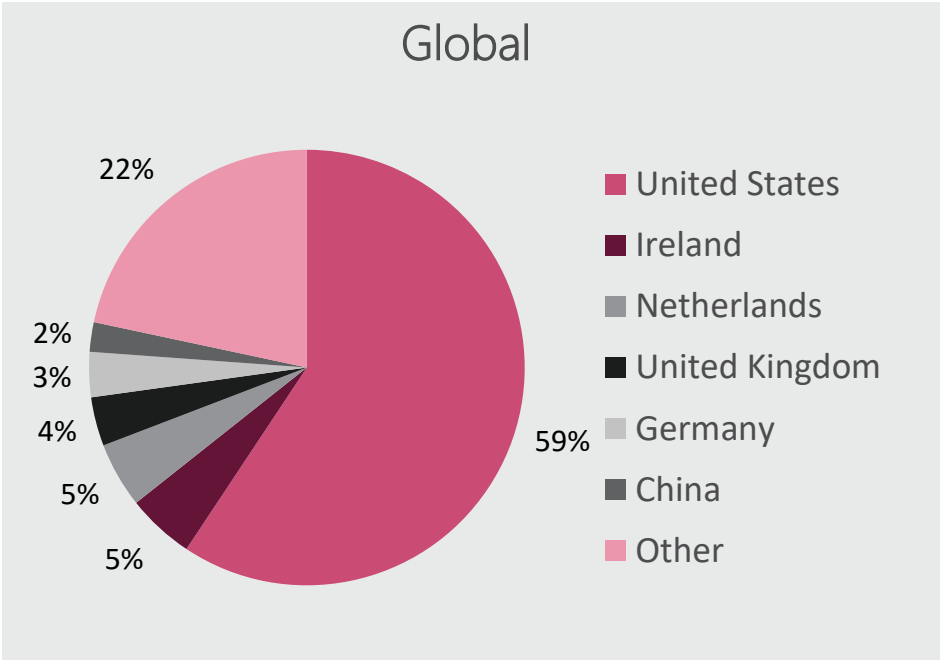
MALWARE FAMILY	COUNTRY IMPACT	GLOBAL IMPACT	DESCRIPTION
Emotet	8%	5%	Emotet is an advanced, self-propagating and modular Trojan that was once used as a banking Trojan, and currently distributes other malware or malicious campaigns. Emotet uses multiple methods for maintaining persistence and evasion techniques to avoid detection and can be spread via phishing spam emails containing malicious attachments or links.
Trickbot	3%	3%	Trickbot is a modular 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.
RigEK	2%	1%	Rig EK was first introduced in April 2014. It has since received several large updates and continues to be active to this day. In 2015, as result of an internal feud between its operators, the source code was leaked and has been thoroughly investigated by researchers. Rig delivers Exploits for Flash, Java, Silverlight and Internet Explorer. The infection chain starts with a redirection to a landing page that contains JavaScript that checks for vulnerable plug-ins and delivers the exploit.
Ursnif	2%	0%	Ursnif is a Trojan that targets the Windows platform. It is usually spread through Exploit Kits, including Angler and Rig in their day. Ursnif steals information related to the Verifone Point-of-Sale (POS) payment software. It contacts a remote server to upload collected information and receive instructions. Moreover, it downloads and executes files on the infected system.
Agenttesla	2%	3%	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.

Top Malware - Global- Jul-20

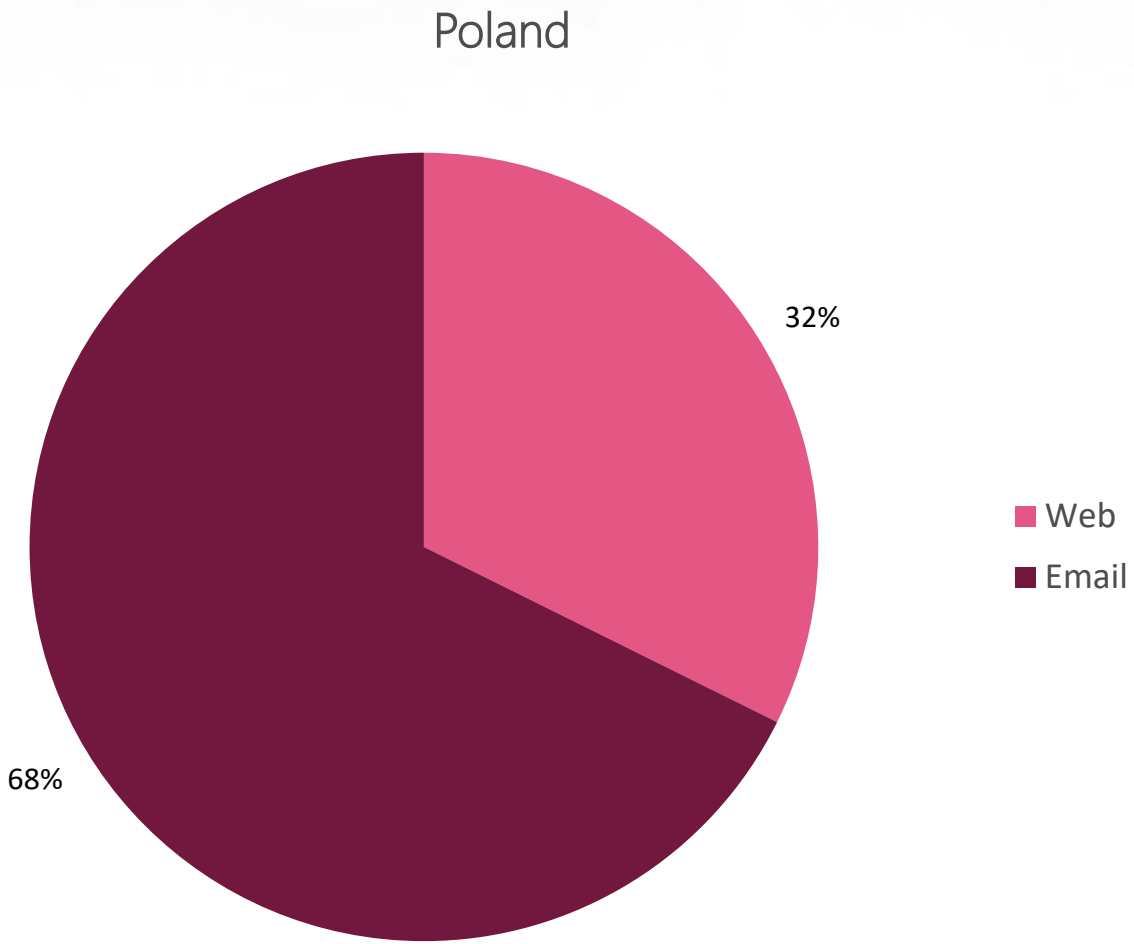
MALWARE FAMILY	GLOBAL IMPACT	DESCRIPTION
Emotet	5%	Emotet is an advanced, self-propagating and modular Trojan that was once used as a banking Trojan, and currently distributes other malware or malicious campaigns. Emotet uses multiple methods for maintaining persistence and evasion techniques to avoid detection and can be spread via phishing spam emails containing malicious attachments or links.
Dridex	4%	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.
Agenttesla	3%	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.
Trickbot	3%	Trickbot is a modular 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	2%	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.

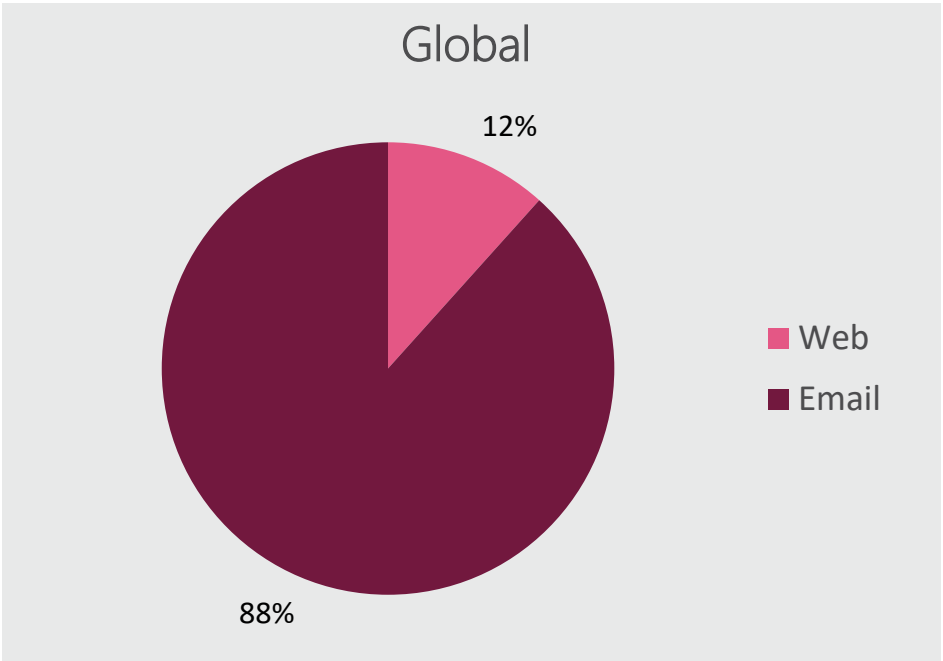
Top Threat Source Countries- Last 6 Months



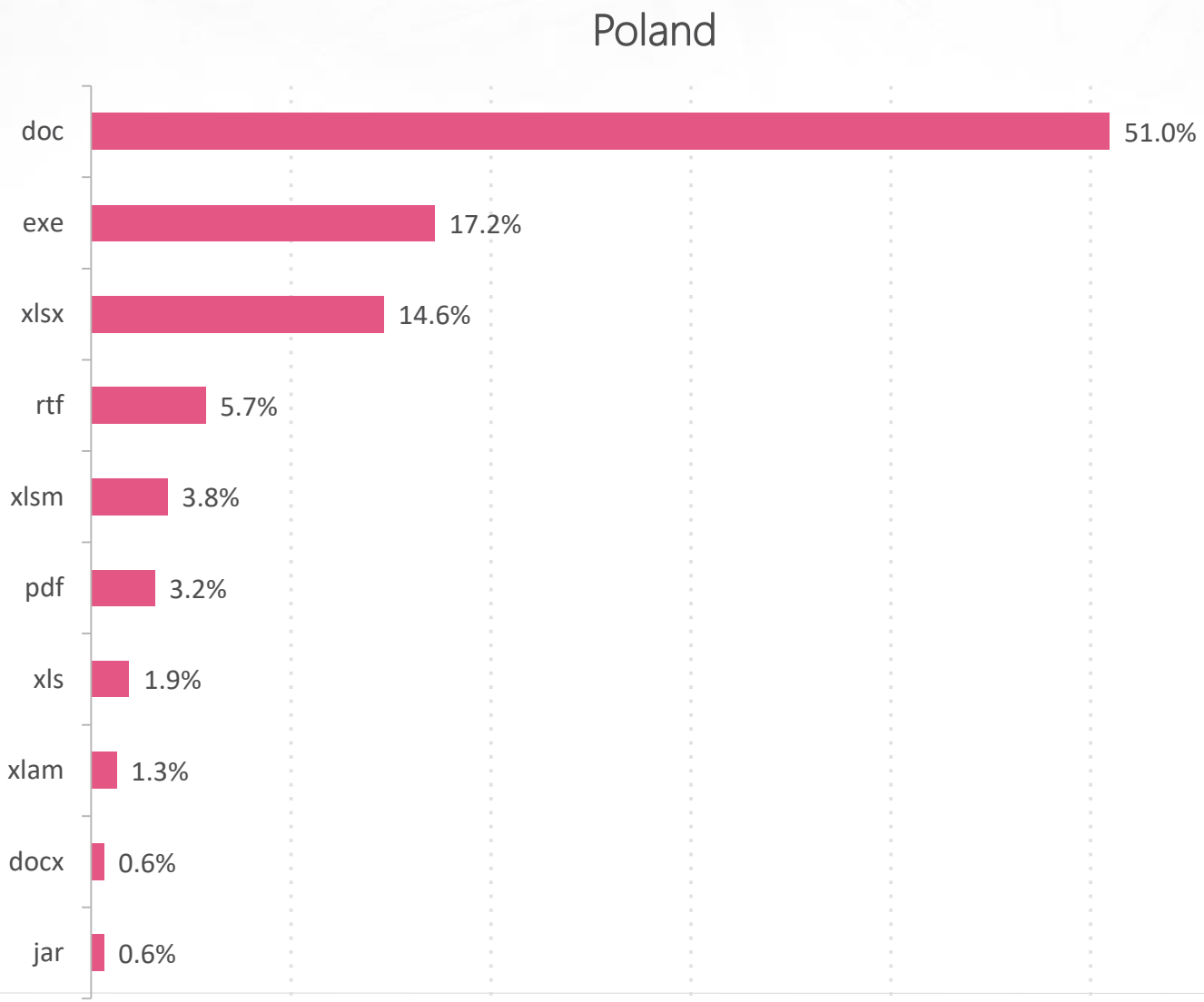


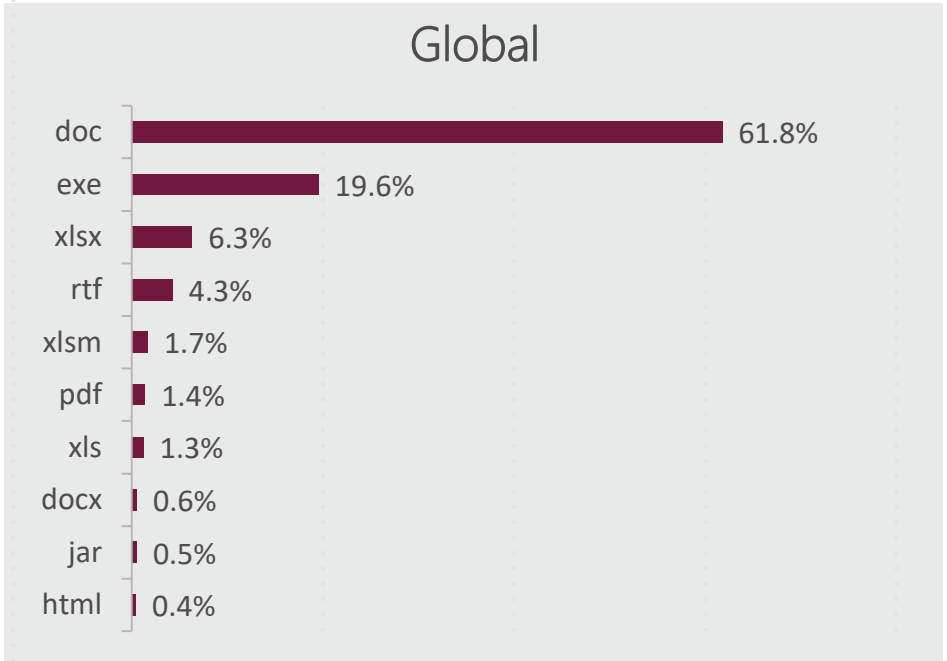
Attack Vectors for Malicious Files- Last 30 Days



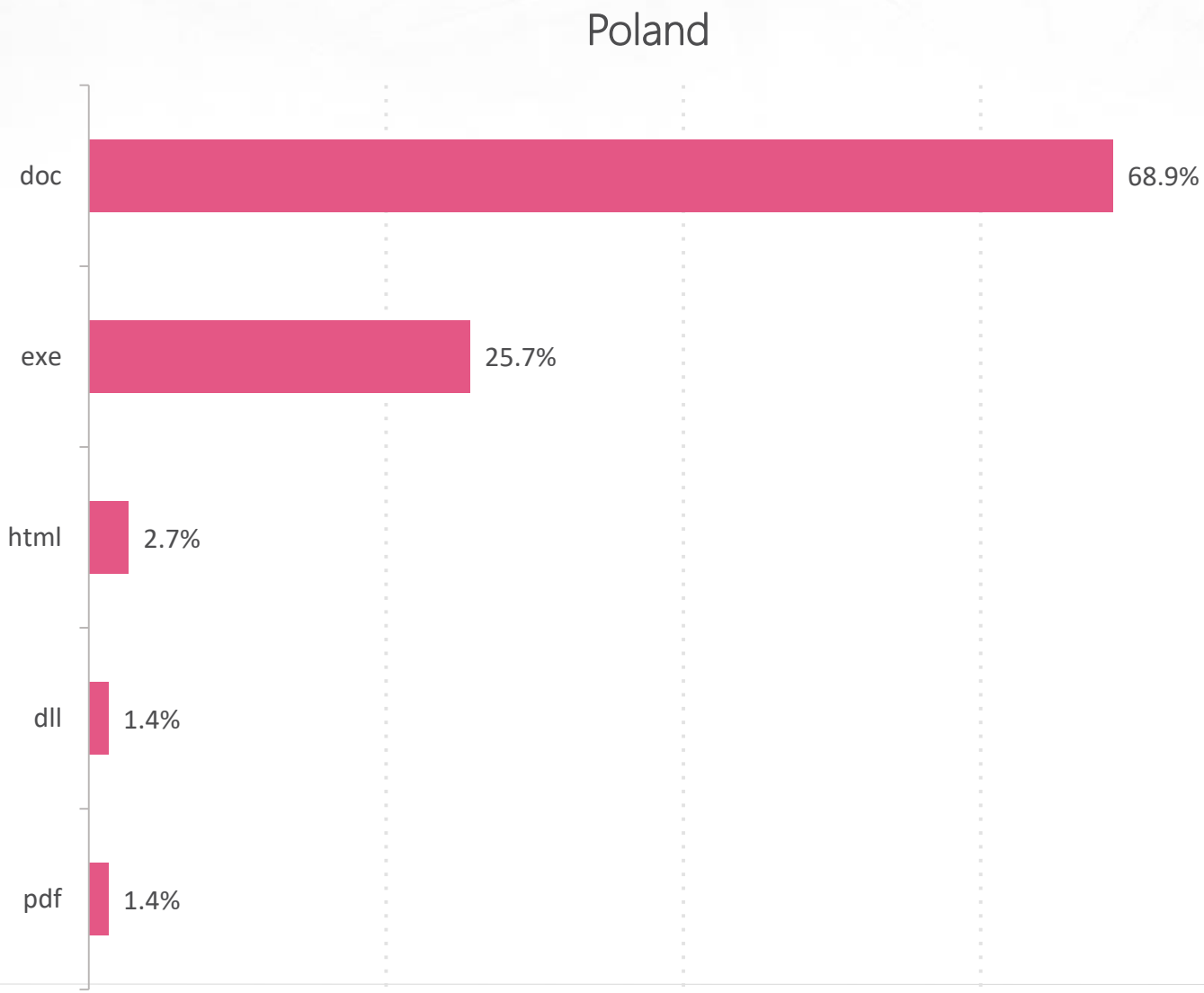


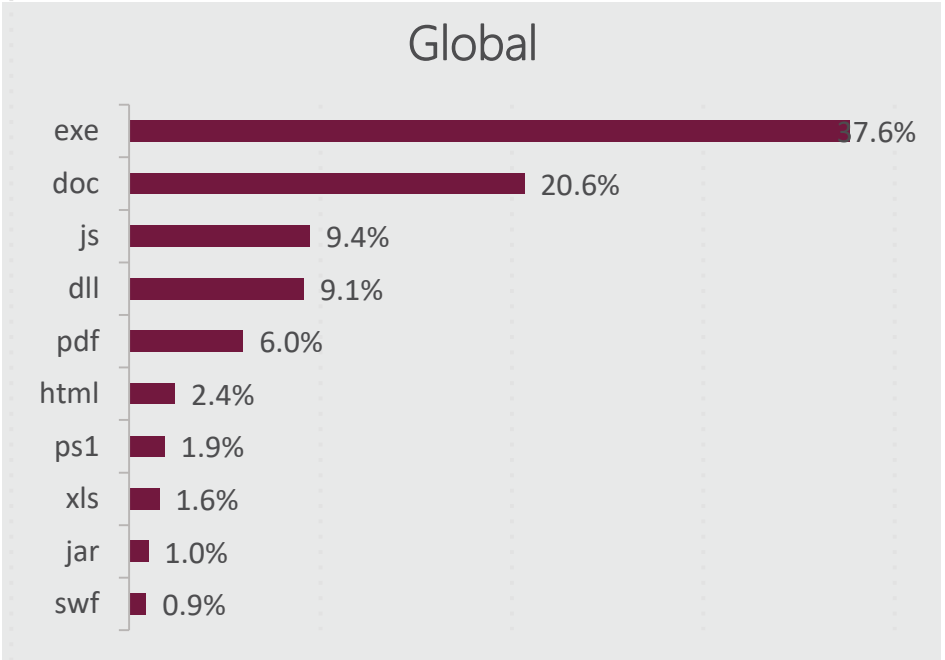
Top Malicious File Types, Email- Last 30 Days



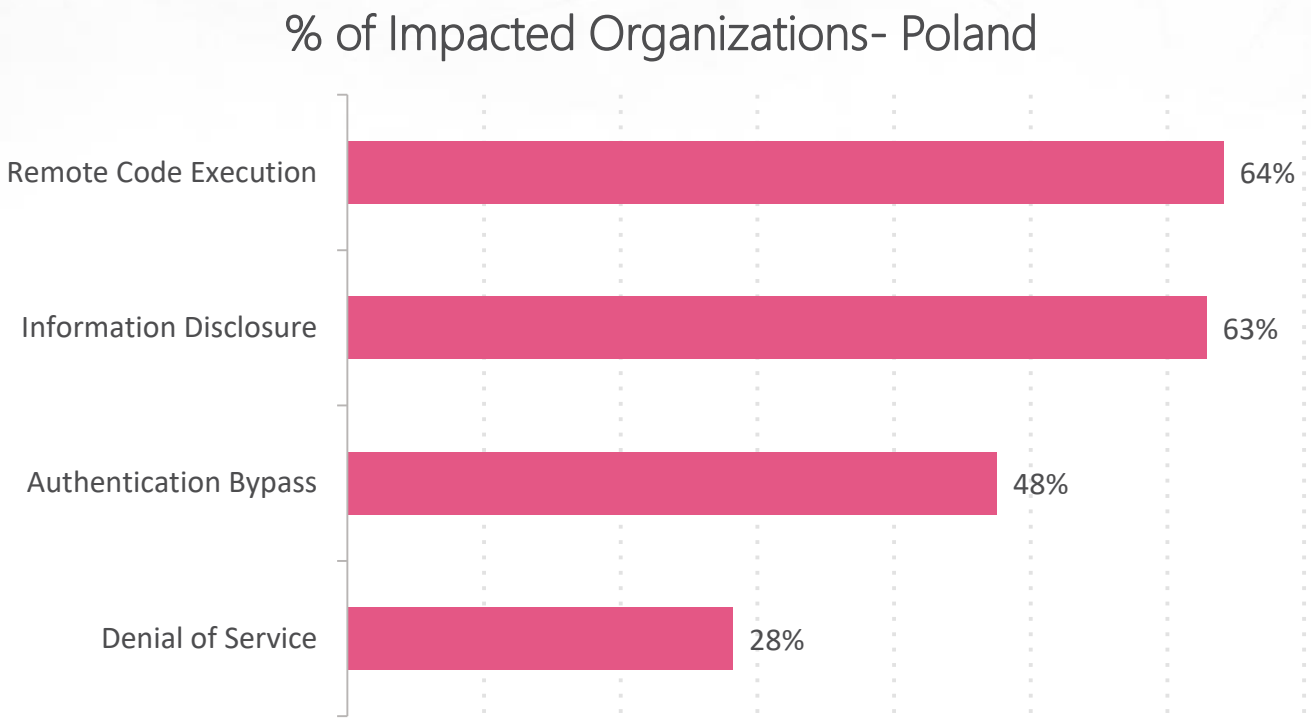


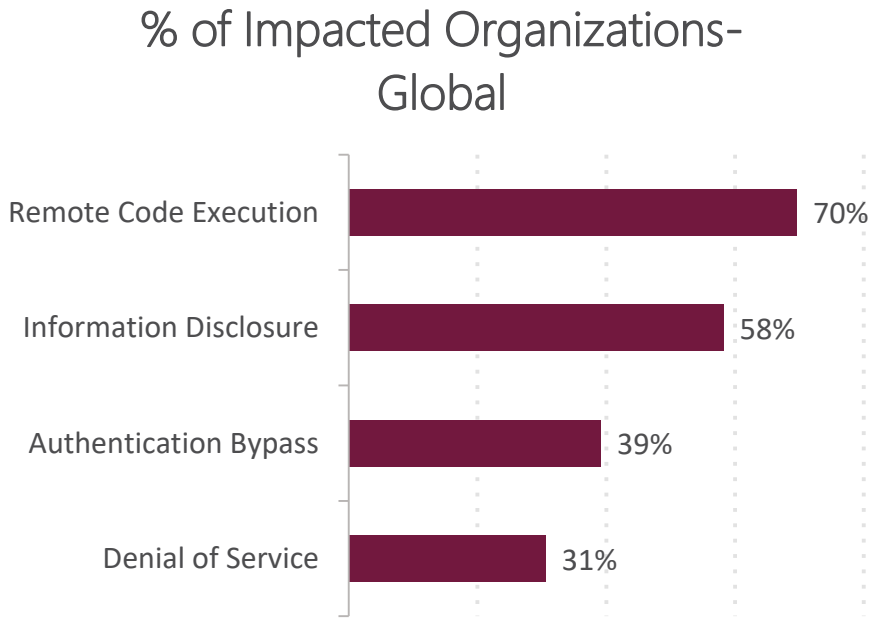
Top Malicious File Types, Web- Last 30 Days



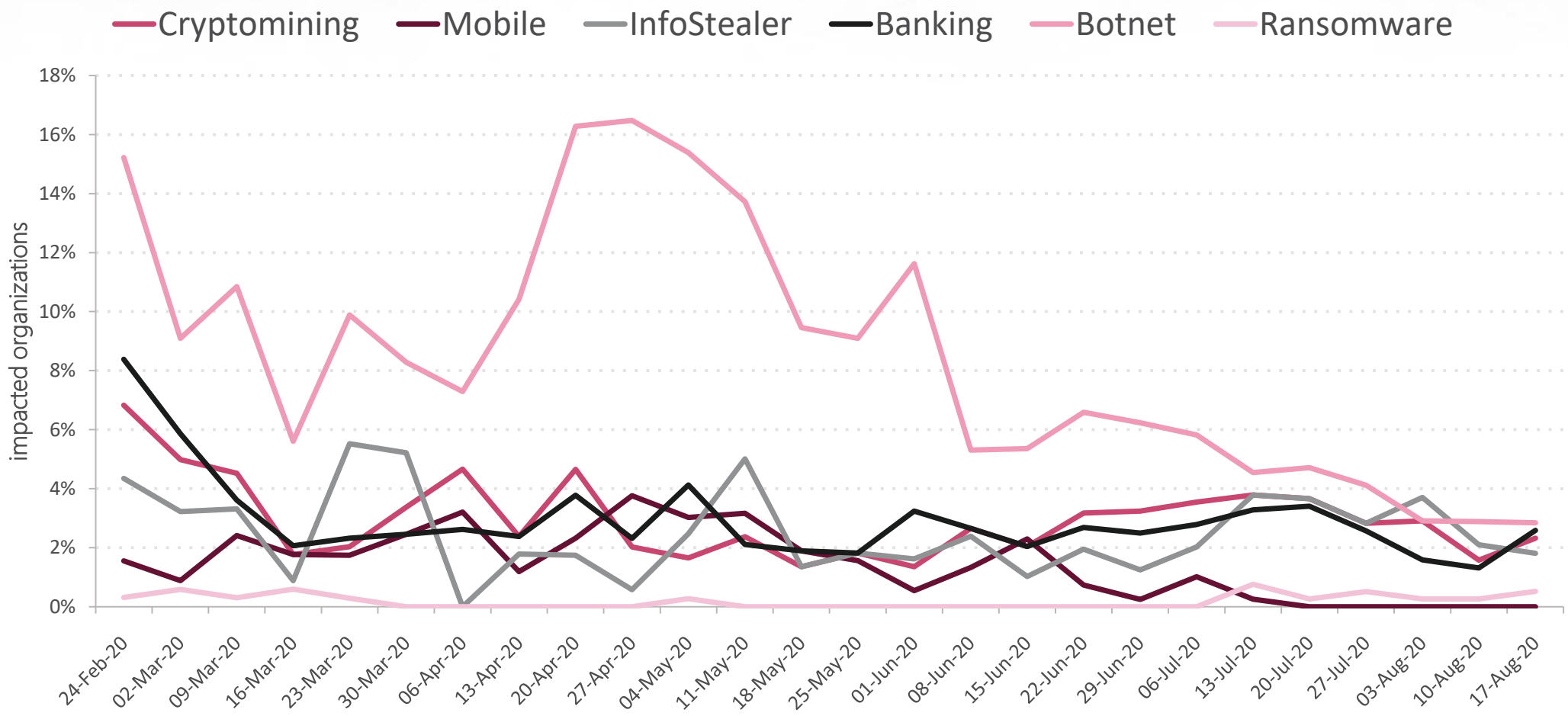


Top Vulnerability Exploit types - Last 30 Days

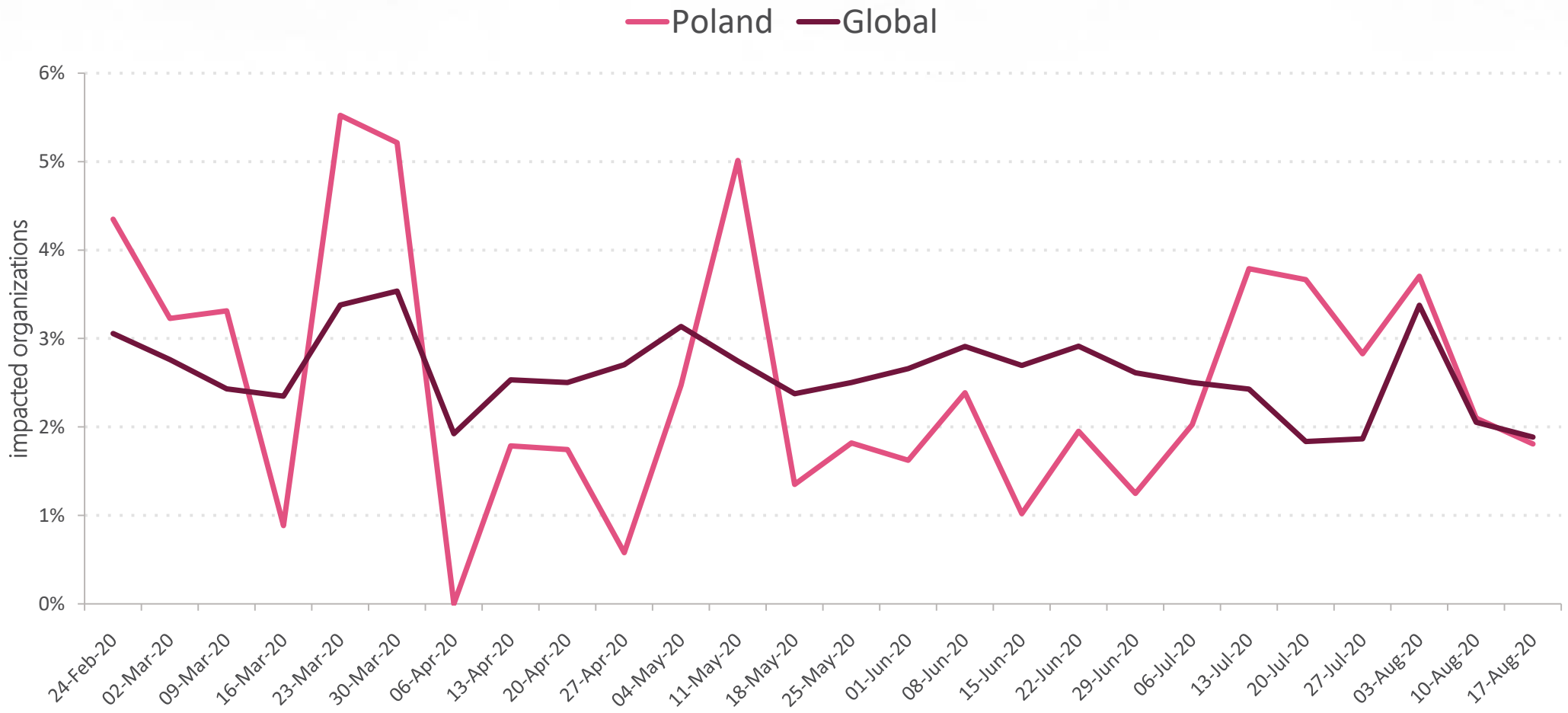




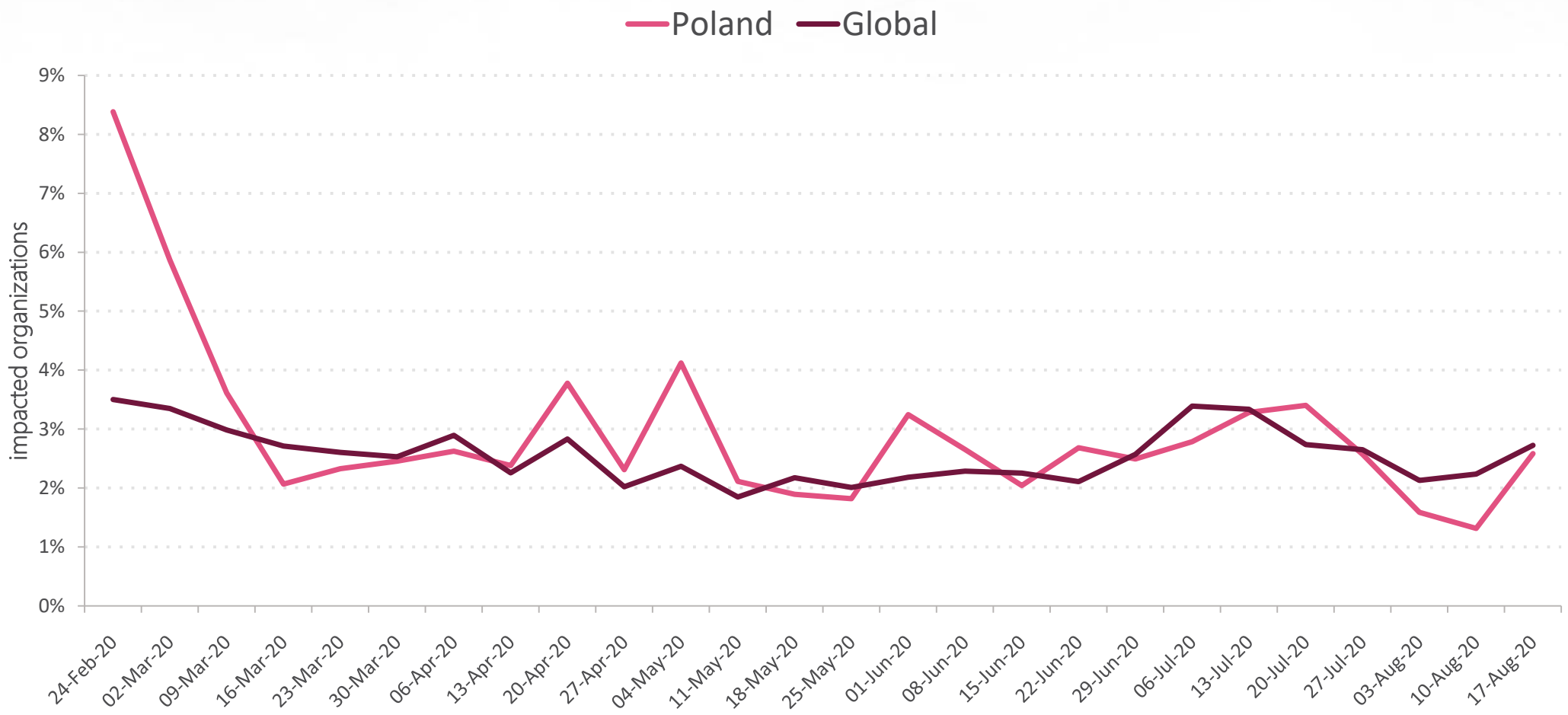
Major Malware Types trend - Last 6 Months



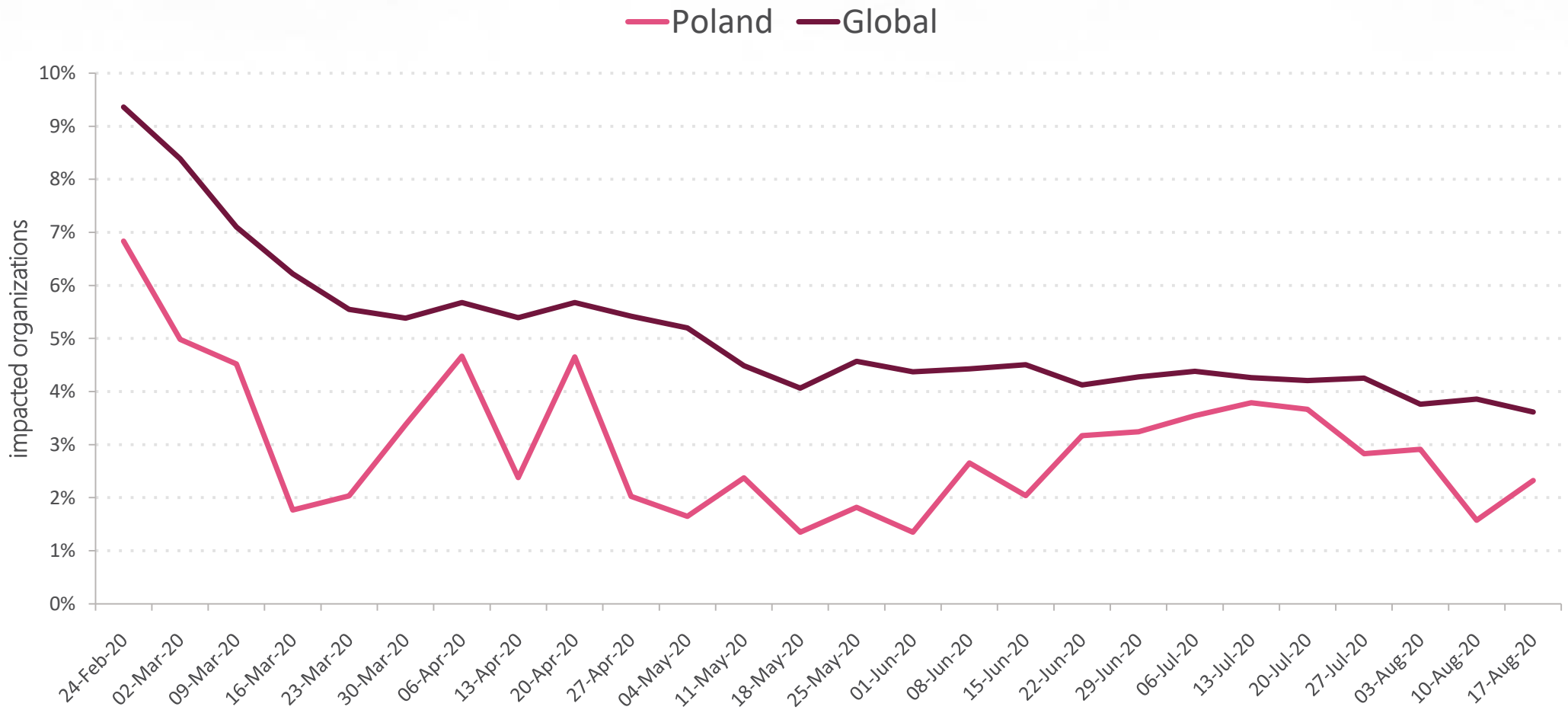
InfoStealer Attacks- Last 6 Months



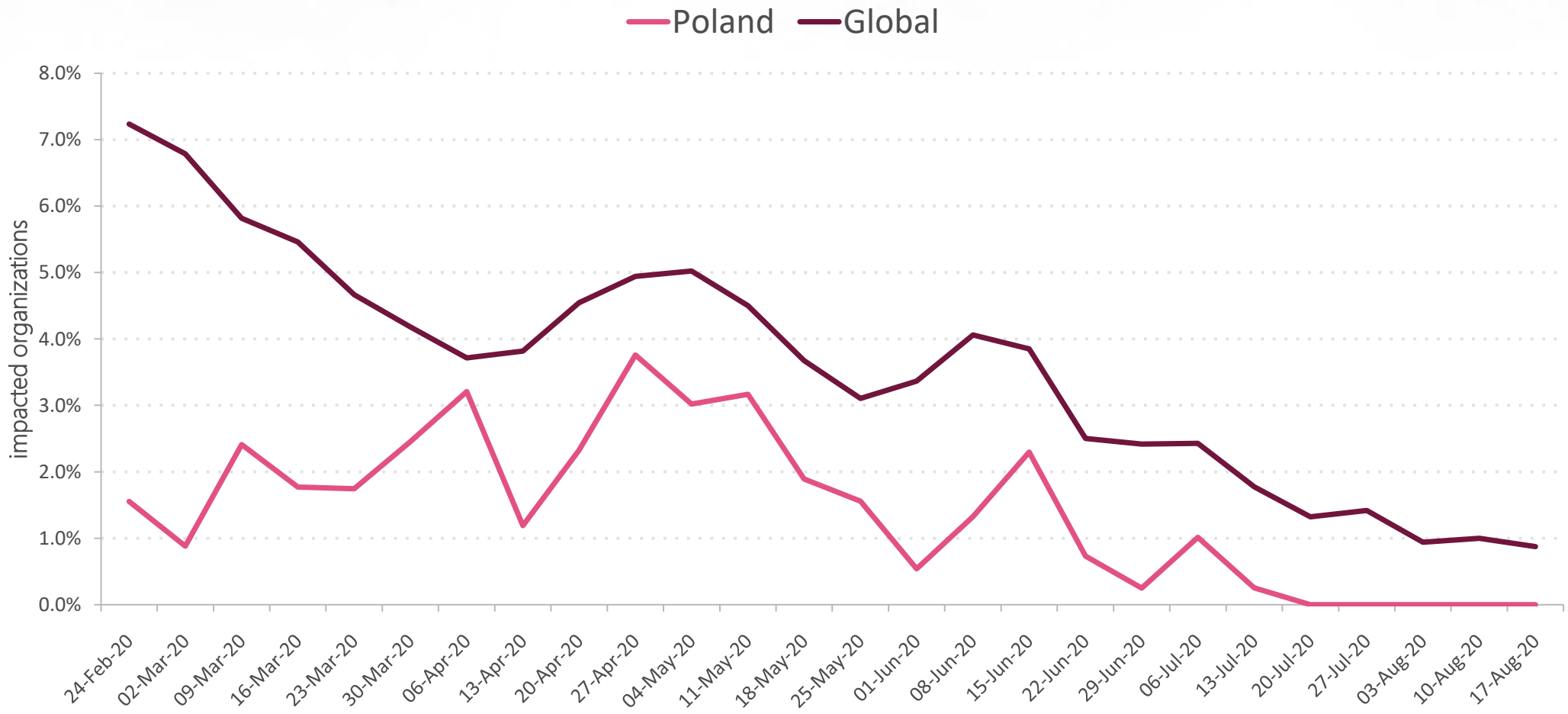
Banking Attacks- Last 6 Months



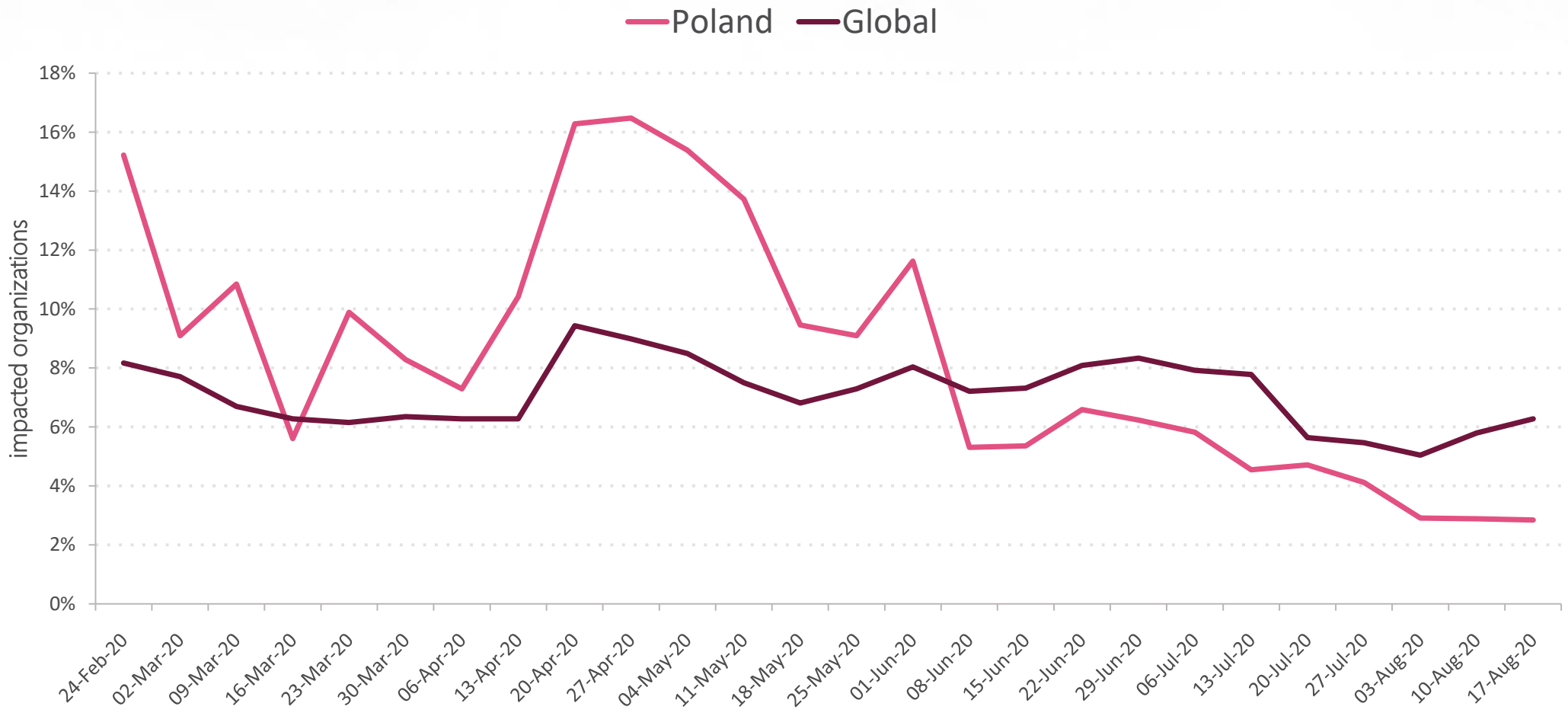
Cryptomining Attacks- Last 6 Months



Mobile Attacks- Last 6 Months



Botnet Attacks- Last 6 Months




Check Point
SOFTWARE TECHNOLOGIES LTD
THANK YOU
More Info:
https://research.checkpoint.com/
cp<r>
CHECK POINT RESEARCH