Unfair exchange: ransomware attacks surge globally amid Microsoft Exchange Server vulnerabilities

Over the past year, hospitals and the healthcare industry have been under tremendous pressure during the COVID-19 pandemic, not only dealing with surges in patient numbers, but also with shameless ransomware attacks launched by cybercriminals who see the sector as a soft target. However, it now seems that criminals are shifting their attention to new targets, because they sense even easier opportunities for their extortion tactics.

Following the recent disclosure of vulnerabilities affecting Microsoft Exchange Servers, Check Point Research (CPR) has observed a global surge in the number of ransomware attacks. In fact, since the beginning of 2021, there has been a 9% increase monthly in organizations affected ransomware. This uptick includes a 57% increase in organizations affected by ransomware in the past 6 months. According to various reports and official alerts from the Cybersecurity and Infrastructure Security Agency (CISA) in the US, ransomware attacks are targeting Microsoft Exchange servers by leveraging previously exposed vulnerabilities.

In the last week alone, the number of attacks involving Exchange Server vulnerabilities has tripled. With over 50,000 attack attempts seen globally, CPR has observed that the most targeted industries are government/military, manufacturing and banking/finance. The most affected country is the United States (49% of all exploit attempts), followed by the United Kingdom (5%), the Netherlands (4%) and Germany (4%).

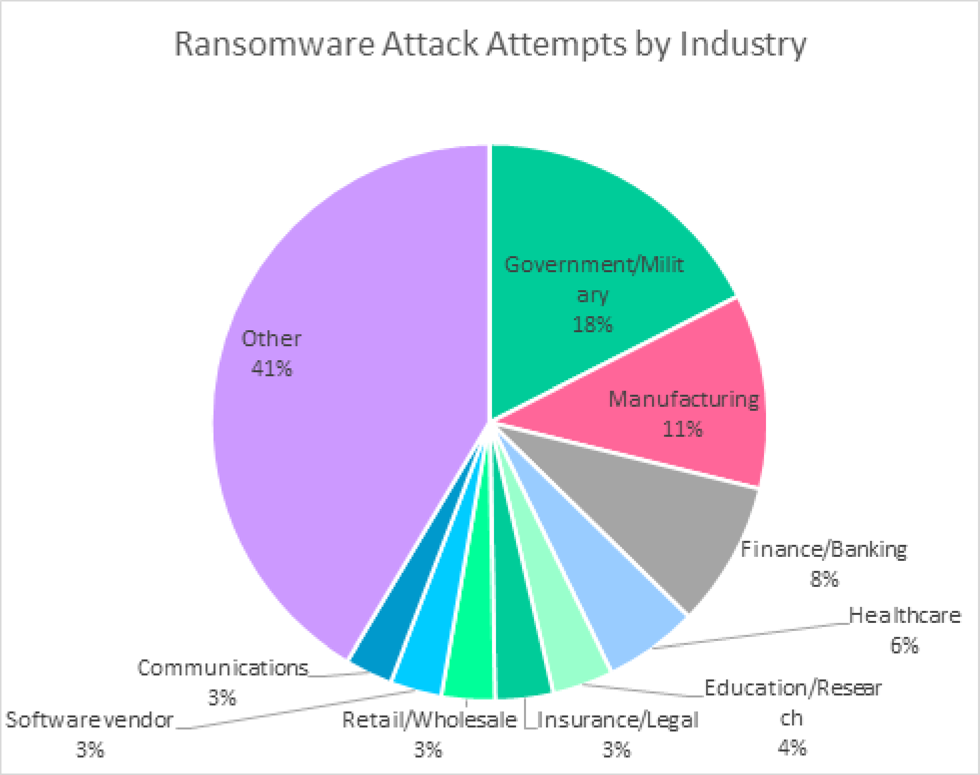
Ransomware spikes globally

CPR has also observed the following trends in ransomware attacks:

- In the past 6 months, there has been a general increase in the number of attacks involving human-operated ransomware, such as Maze and Ryuk, in which victims have to negotiate with the criminals that launched the attack.
- In the last 6 months, there has been a 57% increase in the number of organizations affected by ransomware globally.
- Since the beginning of 2021, the number of organizations affected by ransomware have been growing at 9% monthly.
- In total, 3,868 organizations have been affected with ransomware

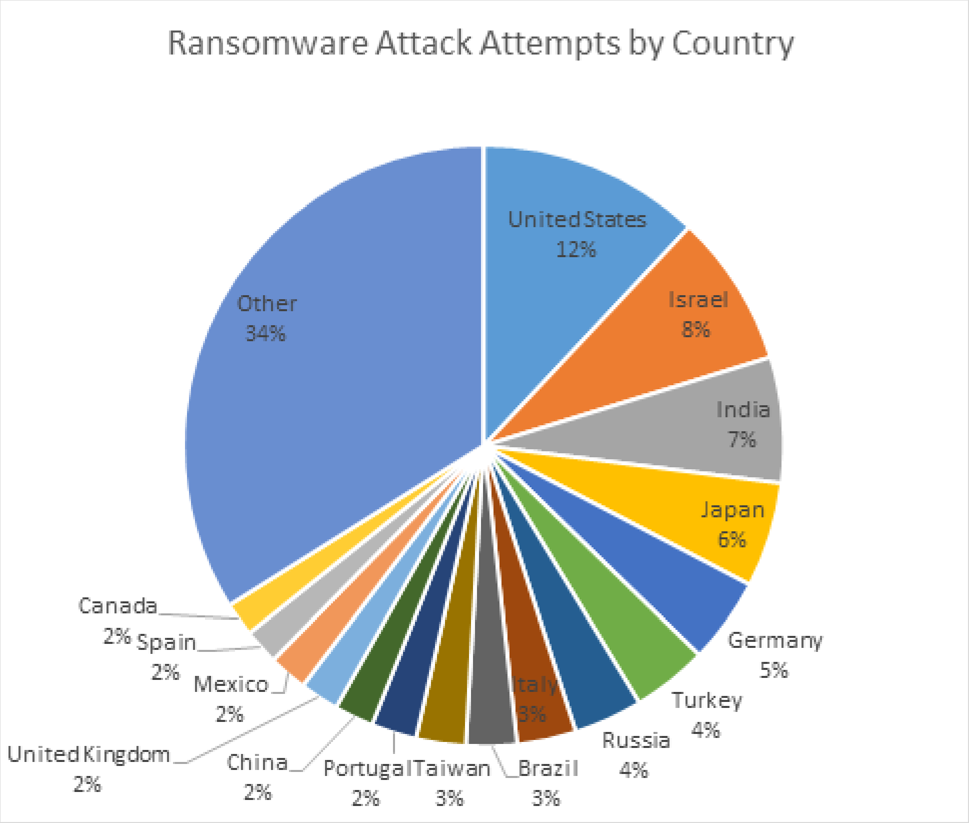
Ransomware Attack Attempts by Industry:

The industry sector most targeted by WannaCry is government/military (18% of total attacks). This is followed by manufacturing (11%), banking and financial services (8%) and healthcare (6%).



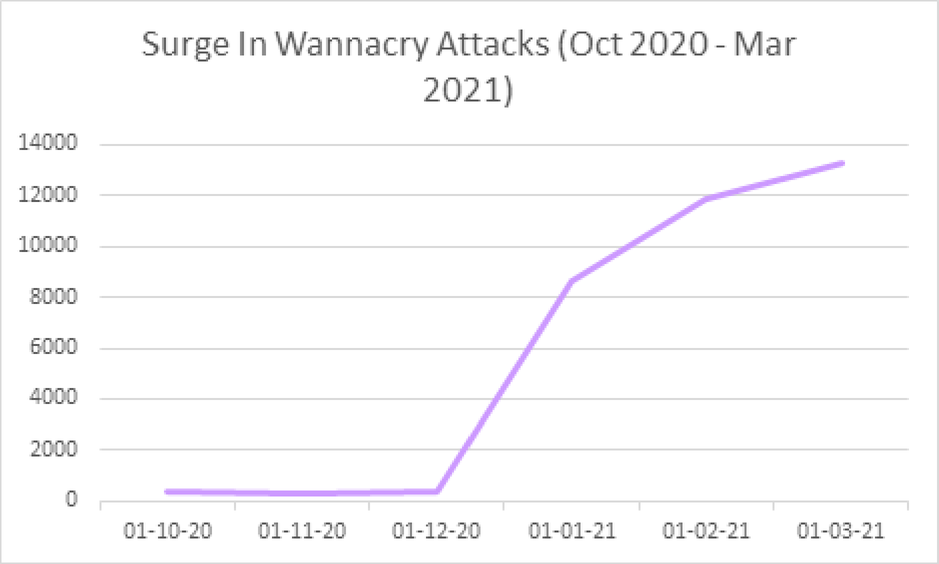
Ransomware Attack Attempts by Country:

The countries most affected by ransomware attack attempts are the United States (12% of all attack attempts), followed by Israel (8%), India (7%) and Japan (6%), while Canada, Spain, Mexico, the United Kingdom, China and Portugal each saw 2%.



WannaCry surges … again!

Worryingly, WannaCry, the wormable ransomware that made its debut four years ago, is also trending again, though it is unclear why. Since the beginning of the year, the number of organizations affected with WannaCry globally has increased by 53%. In fact, CPR found that there are 40 times more affected organizations in March 2021 when compared to October 2020. The new samples still use the EternalBlue exploit to propagate – for which patches have been available for over 4 years. This highlights why it's critical that organizations patch their systems as soon as updates are available.



Ransomware protection for your organization

Below are some fundamental tips to keep your organization protected from ransomware attacks:

- **Back up all data -** One of most important actions to prevent ransomware from disrupting your operations is backing up your company's data regularly. If something goes wrong, you should be able to quickly and easily revert to a recent backup version. This won't actively protect you from being the target of an attack, but if you're ever attacked, the fallout won't be nearly as devastating. Backing up data can help companies avoid having to pay ransom or suffer the ill effects of restoring systems back to a previous version.

- **Keep software updated -** Ransomware attackers sometimes find an entry point within apps and software, noting vulnerabilities and capitalizing on them. Fortunately, some developers actively search for new vulnerabilities and patch them. Adopt a patch management strategy and ensure all team members are constantly up-to-date with the latest versions. As mentioned earlier, WannaCry relies on unpatched systems to spread, yet the patches for the vulnerability it exploits have been available for 4 years – yet evidently many organizations have not applied these updates.

- **Utilize better threat detection -** Most ransomware attacks can be detected and resolved before it's too late. To maximize your chances of protection, have an automated threat detection system in place in your organization.

- **Adopt multifactor authentication -** Multifactor authentication forces users to verify their identities in multiple ways before they're granted access to a system. This way, if an employee mistakenly gives their password to a cybercriminal, the criminal won't be able to gain easy access to your systems.

- Principle of least **privilege (POLP) -** Employees should never have more access to data than they truly need. Segmenting your organization and restricting access can provide a kind of quarantine effect, minimizing the impact of a potential attack and limiting the vectors of access.

- **Scan and monitor emails and file activity -** Emails are the default choice of cybercriminals executing phishing schemes, so take the time to scan and monitor emails on an ongoing basis, and consider deploying an automated email security solution to block malicious emails from ever reaching users. It's also a good idea to scan and monitor file activity. Organizations should be notified whenever there's a suspicious file in play before it becomes a threat.

- **Improve employee training -** Most ransomware attacks are the byproduct of bad employee habits, or pure ignorance. Someone may voluntarily give out their password, or may download an unfamiliar file to their work device. With better employee training, the chances of this happening are much lower.

- **Don't pay the ransom -** Finally, if your organization happens to be the victim of a ransomware attack, don't pay the ransom! It might seem tempting to get out of this bad situation as quickly as possible, but even after paying the ransom, there's no guarantee that the attacker is going to be true to their word.

- **Anti-Ransomware Solutions -** While the previous ransomware prevention steps can help mitigate an organization's exposure to ransomware threats, they do not provide perfect protection. Some ransomware operators use well-researched and highly targeted spear phishing emails as their attack vector. These emails may trick even the most diligent employee, resulting in ransomware gaining access to an organization's internal systems. Protecting against this ransomware that "slips through the cracks" requires a specialized security solution. In order to achieve its objective, ransomware must perform certain anomalous actions, such as opening and encrypting large numbers of files. Anti-ransomware solutions monitor programs running on a computer for suspicious behaviors commonly exhibited by ransomware, and if these behaviors are detected, the program can take action to stop encryption before further damage is done.

The data used in this report was detected by Check Point's Threat Prevention technologies, stored and analyzed in ThreatCloud. ThreatCloud provides real-time threat intelligence derived from hundreds of millions of sensors worldwide, over networks, endpoints and mobiles. The intelligence is enriched with AI-based engines and exclusive research data from the Check Point Research – The intelligence & Research Arm of Check Point.