# We analyzed 80 million ransomware samples – here's what we learned

Oct 13, 2021
Vicente Diaz
VirusTotal

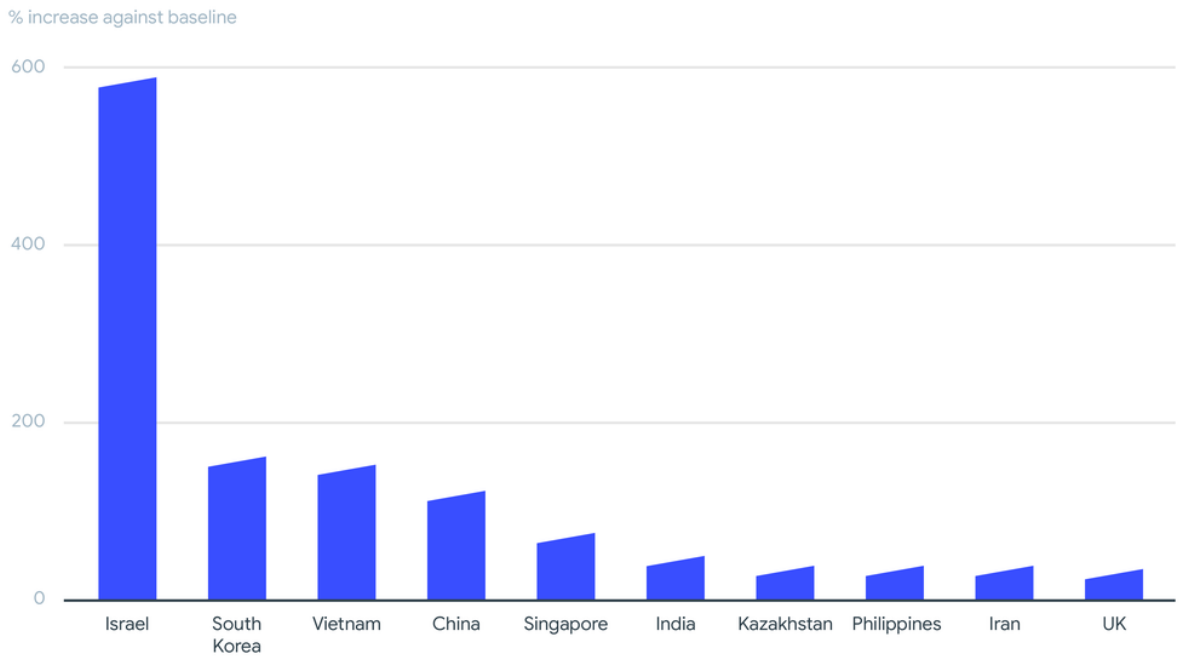
Leaders at organizations across the globe are witnessing the alarming rise of ransomware threats, leaving them with the sobering thought that an attack on their business may be not a matter of if, but when.

The stakes are becoming higher. Hackers aren't just demanding money, they're threatening to reveal sensitive or valuable information if companies don't pay up or if they contact law enforcement authorities. For example, if you run a healthcare organization, the impact can be even more dire - as evidenced by this new report on ransomware attacks that finds attacks against hospitals have resulted in delays in tests and procedures, patients being kept longer, and even death.

One of the main challenges to stopping ransomware attacks is the lack of comprehensive visibility into how these attacks spread and evolve. Leaders are often left with bits and pieces of information that don't add up.

VirusTotal's first Ransomware Activity Report provides a holistic view of ransomware attacks by combining more than 80 million potential ransomware-related samples submitted over the last year and a half. This report is designed to help researchers, security practitioners and the general public understand the nature of ransomware attacks while enabling cyber professionals to better analyze suspicious files, URLs, domains and IP addresses. Sharing insights behind how attacks develop is essential to anticipating their evolution and detecting cybersecurity threats across the globe.

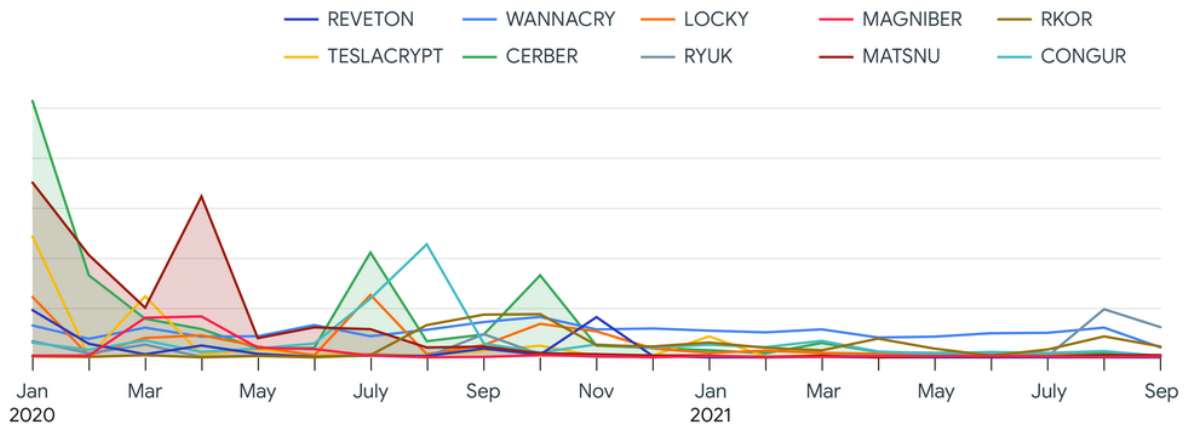
Of the 140 countries that submitted ransomware samples, Israel was far and away an outlier, with the highest number of submissions and nearly a 600 percent increase in the number of submissions compared to its baseline. Israel was followed by South Korea, Vietnam, China, Singapore, India, Kazakhstan, Philippines, Iran and the UK as the most affected territories based on the number of submissions to VirusTotal.




Geographical distribution of ransomware-related submissions

We saw peaks of ransomware activity in the first two quarters of 2020, primarily due to the ransomware-as-a-service group GandCrab (though its prevalence decreased dramatically in the second half of the year). Another sizable peak occurred in July 2021, driven by the Babuk ransomware family – a ransomware operation launched at the beginning of 2021 that was behind the attack on the Washington DC Metropolitan Police Department.

At least 130 different ransomware families were active in 2020 and the first half of 2021 — grouped by 30,000 clusters of malware that looked and operated in a similar fashion. With 6,000 clusters, GandCrab was the most active family - followed by Babuk, Cerber, Matsnu, Congur, Locky, Teslacrypt, Rkor and Reveon.




Activity of 100 most active ransomware families

While these big campaigns come and go, there is a constant baseline of ransomware activity of approximately 100 ransomware families that never stops. Attackers are using a range of approaches, including well-known botnet malware and other Remote Access Trojans (RATs) as vehicles to deliver their ransomware. In most cases, they are using fresh or new ransomware samples for their campaigns. This broad collection of activity provides vital

insights into ransomware growth, evolution and impact on organizations of all sizes, and provides the bread crumbs needed for businesses and governments to be much more proactive in building cybersecurity into their infrastructure.

# How We Are Keeping Organizations Safe From This Threat

At Google, our platforms and products have to be secure by default, and have been designed to keep organizations protected from cybersecurity attacks, including the growing threat of ransomware.

Our Chrome OS cloud-first platform has had no reported ransomware attacks — ever — on any business, education or consumer Chrome OS device. Developed with built-in and proactive security, Chrome OS blocks executables that ransomware often hides in, and system files are kept in a read-only partition ensuring the OS can't be modified by apps or extensions. Additionally, the cloud-first nature of Chrome OS means that your data and files are backed up in the cloud and recoverable if an attack were to happen.

We are committed to offering the industry's most trusted cloud, and have developed solutions that help companies adhere to the five pillars of NIST's Cybersecurity Framework - from identification to recovery. For example, our Cloud Asset Inventory helps businesses identify and monitor all their assets in one place. With email at the heart of many ransomware attacks, Google Workspace's advanced phishing and malware protection provides controls to quarantine emails, defends against anomalous attachment types and protects from inbound spoofing emails. Chronicle, Google Cloud's threat detection platform, allows businesses to find and analyze threats faster within their infrastructure and applications, whether that's on Google Cloud or anywhere else. With engineered-in capabilities and additional solutions, we also make it simple and efficient to respond and recover in the event of an incident.

With better data from crowdsourced intelligence platforms like VirusTotal, decision makers can proactively ensure a more robust range of security solutions are implemented, and that multi-layered approaches to security become standard across all organizations. It's the only way to keep our businesses, schools, hospitals and governments safe against ransomware attacks.

To learn more about how Google can help your organization solve its cybersecurity challenges check out our Google Cybersecurity Action Team.