CyberCube Briefing:

Ransomware Risks & VMware Servers

CyberCube

CyberCube advises (re)insurers on ransomware risks to outdated VMware servers

The ongoing automated ransomware campaign ESXiArgs is targeting outdated VMware ESXi hypervisors installed on servers around the world. The first reports of ESXiArgs surfaced on Friday, February 3rd, 2023, and within days, internet-wide scans show a rapid infection rate with thousands of servers infected.

This report aims to advise the (re)insurance and broking industry on the developments to date and what actions they should take to advise their clients.

Executive Summary

- A new automated ransomware campaign called ESXiArgs is targeting outdated VMware ESXi servers globally. The campaign encrypts configuration files on vulnerable ESXi servers, potentially rendering clients' virtual machines unusable. Internet-wide scans within days after the first reports surfaced showed a rapid infection rate with over 2,000 servers infected.

- The majority of impacted ESXi servers are in France and Germany, managed by cloud hosting providers OVHcloud and Hetzner, respectively. The Georgia Institute of Technology in Atlanta, Rice University in Houston, and institutions of higher learning in Hungary and Slovakia have also been impacted, along with Florida's Supreme Court.

- CyberCube has analyzed companies in its Industry Exposure Database (IED) to identify organizations running VMware ESXi hypervisors that could be vulnerable to the ESXiArgs ransomware. Large US-based insureds operating in banking, education, manufacturing, non-profit, aviation, and agriculture are at higher risk of being attacked by threat actors leveraging vulnerabilities in ESXi hypervisors compared to insureds operating in other industries.

- The potential impact of the attack is yet to be fully determined. CyberCube has modeled a large-scale ransomware attack on cloud services providers as part of *Portfolio Manager*, a scenario-based data-driven cyber-disaster modeling solution for (re)insurance professionals.

What is happening?

The ongoing automated ransomware campaign ESXiArgs is targeting outdated VMware ESXi hypervisor servers around the world. Up to 70,000 ESXi hypervisors could be vulnerable.

VMWare ESXi is a hypervisor — software that creates and runs virtual machines (VMs) on servers — that VMware sells to cloud hosts and other large-scale enterprises to consolidate their hardware resources by hosting several VMs running multiple operating systems on a single physical server.

VMware ESXi servers can support multiple installations of the same or different Operating Systems in isolated environments and one ESXi server can run up to 128 virtual Central Processing Units (CPUs) and 120 Virtual Machines (VMs), multiplying impacted entities.

The vulnerability (CVE-2021-21974) affects ESXi 7.0, 6.7 and 6.5. Support for ESXi 6.7 and 6.5 ended in October 2022. The flaw was disclosed, and a fix was released in February 2021.

Countries impacted to date

Both France and Italy's Computer Emergency Response Teams (CERTs) have issued alerts warning of attack campaigns targeting VMware ESXi hypervisors with the aim of deploying ransomware on them.

The majority of impacted ESXi servers are in France and Germany; these servers are mainly being run and managed by cloud hosting providers OVHcloud and Hetzner, respectively. Notably, OVH is a French multinational enterprise providing cloud hosting services.

Cybersecurity agencies in smaller countries, including Singapore, have also raised alarms. At least a dozen universities have been reported to be impacted, including the Georgia Institute of Technology in Atlanta, Rice University in Houston, and institutions of higher learning in Hungary and Slovakia. Florida's Supreme Court has also stated that it was impacted by ESXiArgs ransomware.

While many devices were encrypted, the initial ESXiArgs campaign has been largely unsuccessful as threat actors failed to encrypt flat files, where data for virtual disks are stored. This increases the chances of recovering enough data to rebuild the virtual machine without decryption.

However, starting on 2/9/2023 the cybersecurity community saw threat actors improve the attack with more success. Newer versions of ESXiArgs are less recoverable than previous strains. Victims in the second wave of attacks are likely going to be forced to pay a ransom.

CyberCube helps identify vulnerable companies

CyberCube has analyzed companies in its Industry Exposure Database (IED) to identify organizations running VMWare ESXi hypervisors that could be vulnerable to the ESXiArgs ransomware. CyberCube's IED is a representative portfolio of insurable US entities expected to carry stand-alone cyber insurance.

Large US-based insureds operating in banking, education, manufacturing, non-profit, aviation, and agriculture are at higher risk of being attacked by threat actors leveraging vulnerabilities in ESXi hypervisors compared to insureds operating in other industries. These six industries displayed the highest concentration of ESXi hypervisors, which means that these industries are likely to have more legacy versions of ESXi that are vulnerable to exploitation and subsequently to ESXiArgs ransomware.

Large insureds ($1 billion-plus revenue) are at greater risk of being impacted than medium, small, or micro-sized insureds. Large-sized companies are more likely to require the use of hypervisors and virtual machines as the foundation for the large-scale deployment of cloud computing and cloud storage resources.

Insureds that rely on legacy ESXi infrastructure including versions that are unpatched and/or end-of-life in all sectors are at risk. Furthermore, VMware as a platform and ESXi are complex products to manage from a security perspective. Underwriters should pay attention to organizations that operate on thin margins and have smaller budgets for IT resources and updates, newer versions, and software patches.

CyberCube customers can use *Single Point of Failure (SPoF) Intelligence* to help determine if companies in a portfolio are using virtual machines on ESXi hypervisors that are maintained by a third-party cloud provider. These companies are at risk of having their ESXi server-based data stolen and encrypted by EXSiArgs ransomware.

The potential impact

While it is too early to determine the full impact of this large-scale ransomware attack, similarities can be drawn to Kaseya VSA in July 2021. The REvil group exploited a vulnerability in Kaseya's VSA remote management software to distribute ransomware to the software's users, affecting hundreds of businesses and organizations around the world. It is considered to be one of the largest ransomware attacks in history by the number of unique entities impacted.

The impact of the ESXiArgs ransomware attacks is still being tallied. However, given the attacks have already encrypted data on thousands of servers that each could contain up to 120 VMs, this attack is starting to look like it could end up being comparable to (or worse than) Kaseya.

How can cyber reinsurers and brokers prepare for similar events?

CyberCube has modeled a large-scale ransomware attack as part of *Portfolio Manager*, a scenario-based data-driven model that enables risk professionals to develop insights for their senior leadership and teams. It also allows stress testing of portfolios of insurance risk so that loss drivers and areas of accumulation risk can be identified.

CyberCube models several outage scenarios for major cloud service providers (CSPs). In Scenario 37 — one of the most devastating scenarios — threat actors attack a major CSP with ransomware. Insureds are unable to access hosted environments, storage, and/or data to varying degrees and experience downtime until restored.

CyberCube's single-risk broking and underwriting solutions can help identify companies that tolerate outdated and End-of-Life (EOL) software products like the vulnerable versions of ESXi being targeted in this attack. Companies that tolerate large amounts of EOL products are vulnerable to other threat actors exploiting known vulnerabilities to achieve network access.

Conclusion

The potential list of vulnerable ESXi hypervisors will likely be exhausted quickly by attacks made by the ESXiArgs ransomware operators, especially as organizations learn of the attack and prioritize patching, meaning the number of vulnerable ESXi hypervisors will go down.

A key lesson learned from ESXiArgs is that one attack could conceivably shut down entire data centers and affect virtualized storage shared among critical workloads, with devastating effect. While this has not been the case so far with ESXiArgs ransomware, the potential for threat actors to cause more damage is real and rising.

We now know that it is possible for threat actors to craft an automated ransomware attack that strikes thousands of unpatched servers in a matter of days. In the future, we could see threat actors innovate to include previously undisclosed zero-day vulnerabilities in this type of attack to target up-to-date versions of critical cloud infrastructure such as VMWare ESXi hypervisors.

Author

William Altman, Cyber Threat Intelligence Principal

Editorial Manager

Yvette Essen, Head of Content, Communications & Creative

Designer

Muhammad Ahmad, Graphic Designer

CyberCube

www.cybcube.com