# Ransomware-&-CVE: Industry Insights Into Exclusive High-Value Target Adversarial Datasets

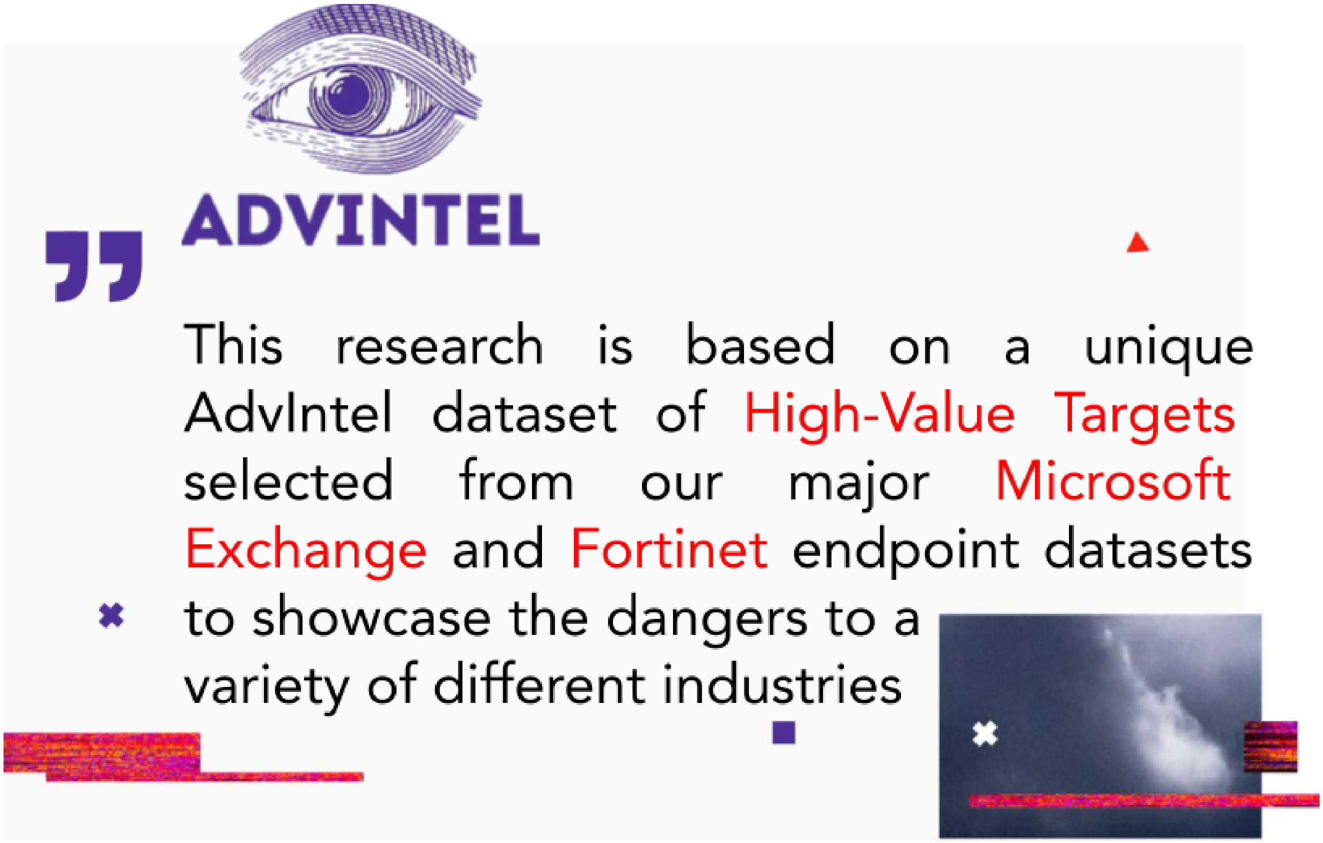
advanced-intel.com/post/adversarial-perspective-advintel-breach-avoidance-through-monitoring-initial-vulnerabilities

AdvIntel June 29, 2021

- Jun 29, 2021
-
- 8 min read

***By Yelisey Boguslavskiy, Brandon Rudisel & AdvIntel Security & Development Team***

*Four months ago two major vectors of vulnerabilities - MS Server vulnerability and Fortinet vulnerability started to be exploited by ransomware groups. Through these months extensive patching and timely updates helped to reduce the threat, but the risk still exists. In these datasets Advanced Intelligence, LLC offers a brief data visualization summary of the Ransomware-&-CVE threat landscape.*



This research is based on a unique AdvIntel dataset of High-Value Targets selected from our major Microsoft Exchange and Fortinet endpoint datasets to showcase the dangers to a variety of different industries

## Introduction

This research is based on a unique AdvIntel dataset of High-Value Targets selected from our major **Microsoft Exchange** and **Fortinet endpoint datasets** to showcase the dangers to a variety of different entities.

Besides botnets and direct DarkWeb access, the most common vectors of initial attacks for ransomware groups **are either system CVEs or infrastructural vulnerabilities**. To represent the two latter attack vectors, AdvIntel focused on the two most representative datasets - Microsoft Exchange Server vulnerabilities for the CVE segment of attack and Fortinet VPN exposure for infrastructure vulnerabilities. The two types of exposures were selected based on an adversarial perspective - AdvIntel's DarkWeb monitoring identified that these two types of vulnerabilities were the most discussed across the criminal underground. The discussions were performed on forums and chat groups especially favored by the ransomware syndicates.

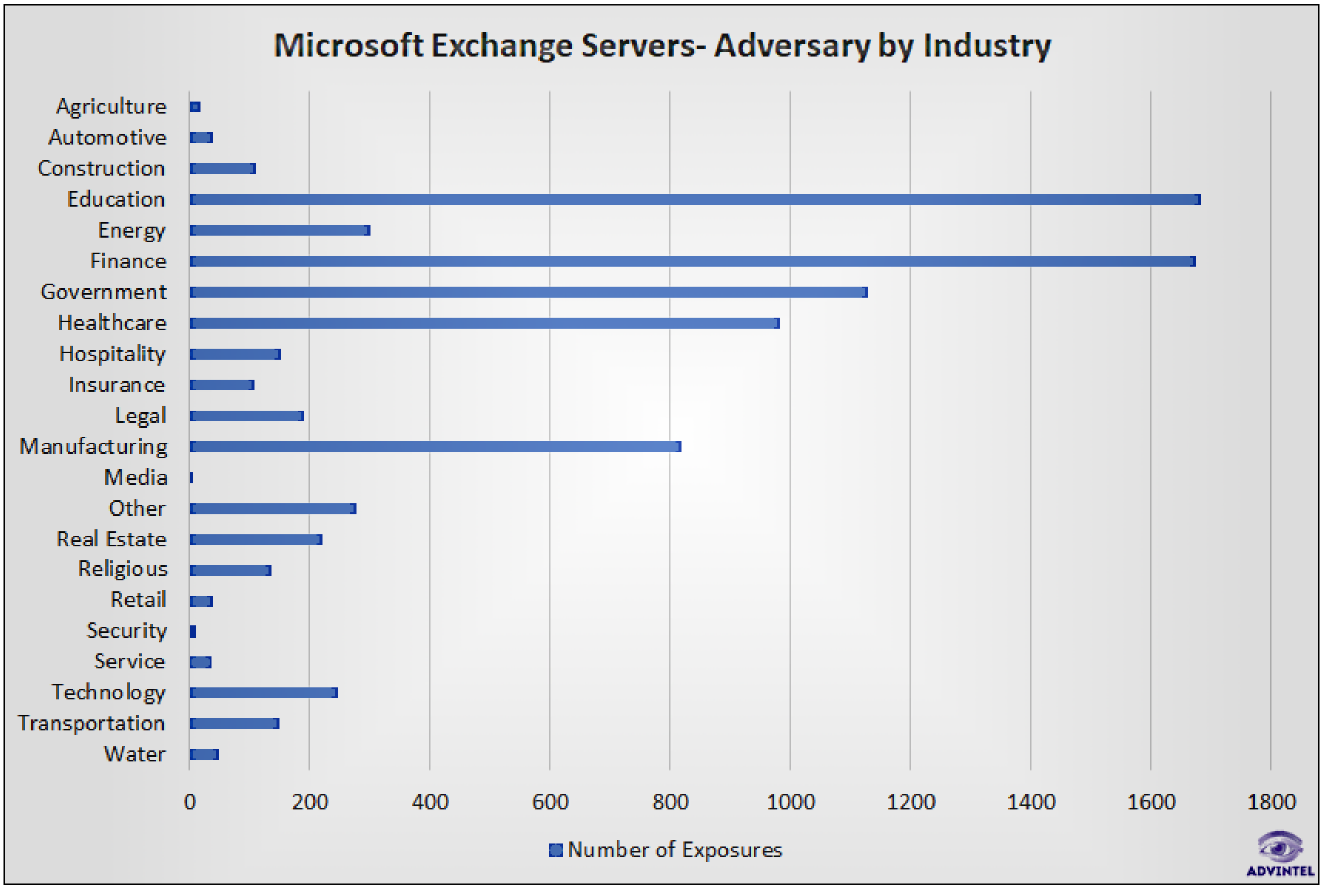
**The full visibility of AdvIntel HVT sets is available in AdvIntel Andariel.**

**Industries Statistical Analysis**

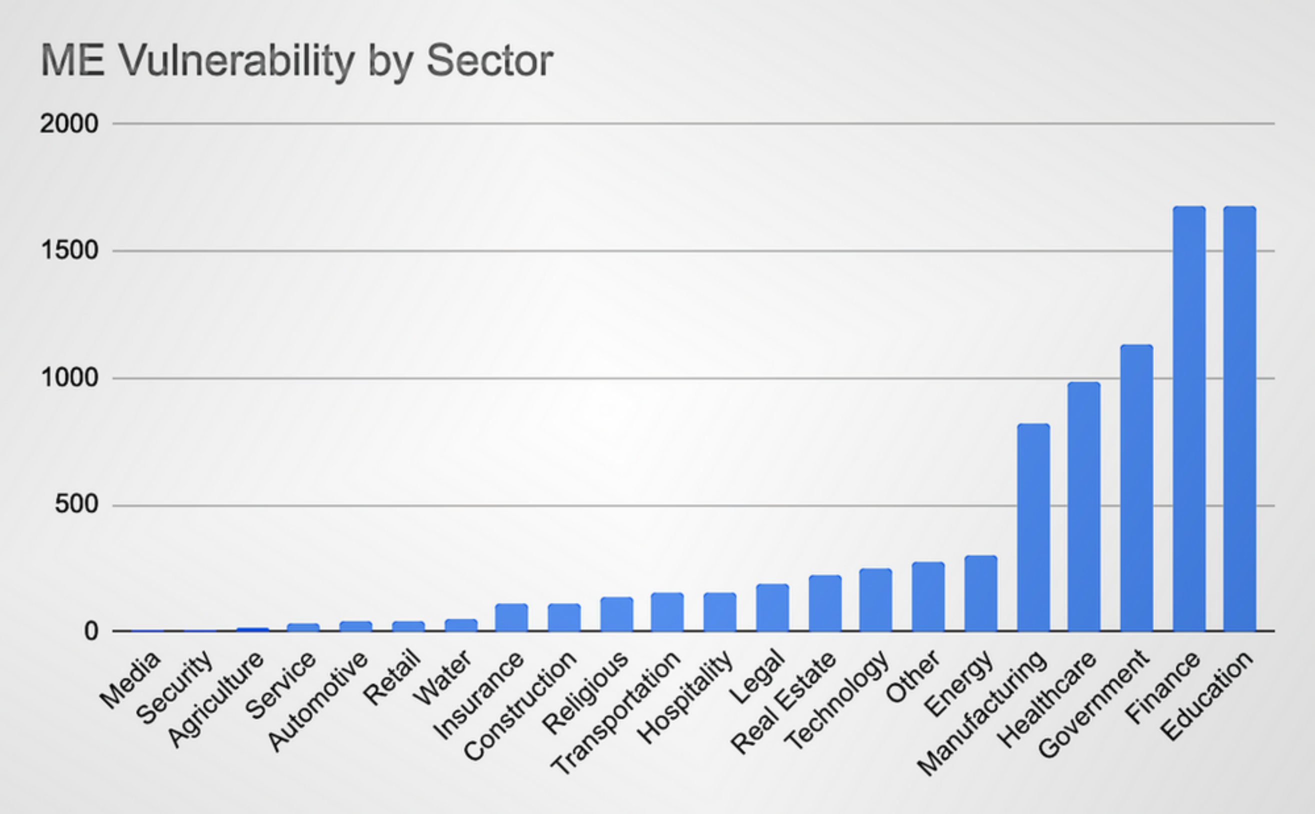
- **The Microsoft Exchange - Adversarial dataset** consists of **8,390 HVT** companies from the original 2,506,718 collected from AdvIntel's Andariel Platform.
- Next, AdvIntel selected **771 HVT** companies from the original **79,128** collected for the **Fortinet/Fortigate** VPN exposure due to it being a popular attack vector for many ransomware groups and nation-state advanced persistent threat (APT) groups.
- The sample size for both data sets was chosen utilizing a rigorous process, ensuring an adequate sample size, enabling AdvIntel to reach an accurate conclusion regarding the represented industries.
- ***Note:*** *Some of the HVT targets were present in several categories. For instance, a religious school would be reported in both Education and Religious statistics.*

**Microsoft Exchange Server CVEs – Overall Adversarial Dataset**: AdvIntel data analysis resulted in ***21 industry categories***, with a few outliers falling under the "other" category. The top five industries exposed were education with **1,683**, finance with **1,675**, government with **1,129**, healthcare with 984, and manufacturing with **819**.

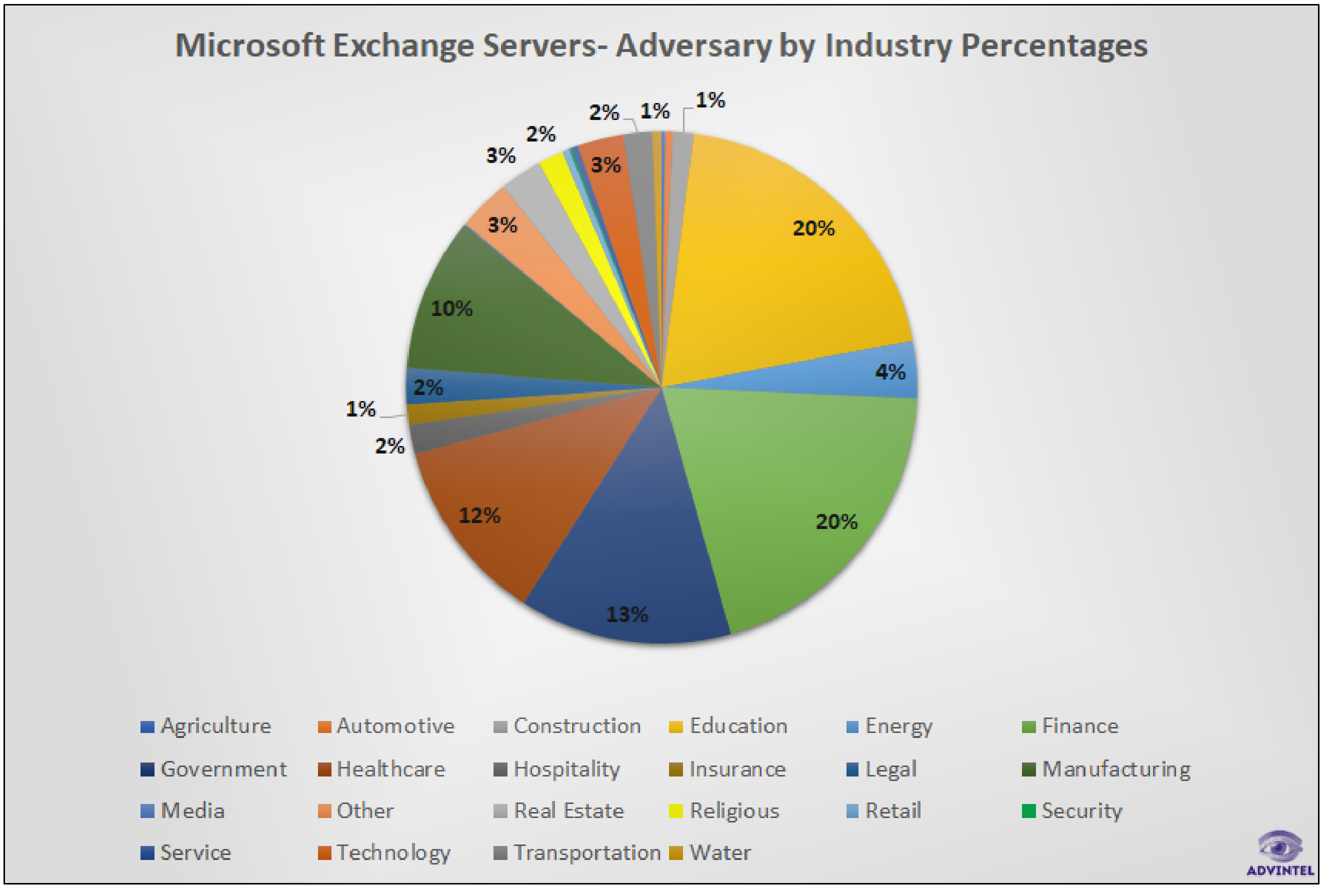
The top five industries consisted of 75% of all exposures for the Microsoft Exchange Adversarial data set. This large percentage highlights how important it is for companies and organizations belonging to these specific industries to take preventative measures to protect themselves. If immediate steps are not taken it could result in threat actors conducting malicious operations against them.



*Data Source: AdvIntel HVT Dataset - Microsoft Exchange Vulnerability*

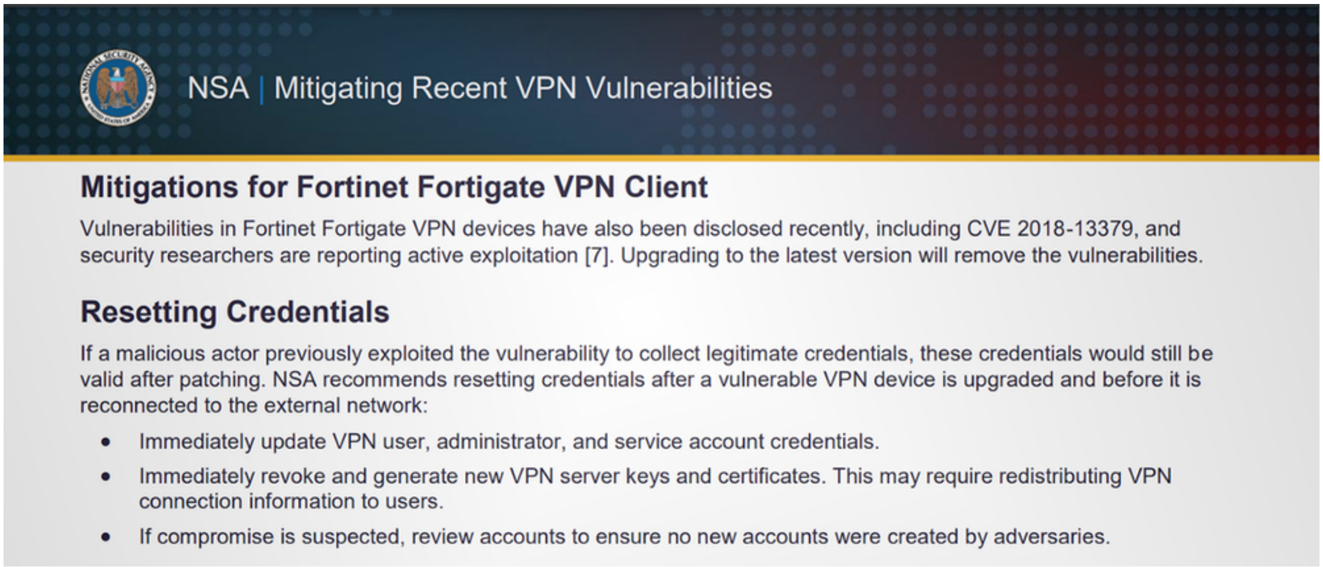


**Fortinet VPN Gateways**: Data analysis resulted in ***22 industry categories*** with multiple exposures, while the remaining industries fell into the "other" category. The top five industries exposed were service with **234**, government with **111**, finance with **110**, manufacturing with **83**, and education with **73**.



Analysis shows the top five industries consisted of 78% of all exposures for the Fortinet VPN gateways data set. This attack vector is popular with ransomware groups and could be utilized to perform malicious actions against unprepared organizations.

## Fortinet VPN Case Study & Industry Review



NSA | Mitigating Recent VPN Vulnerabilities

## Mitigations for Fortinet Fortigate VPN Client

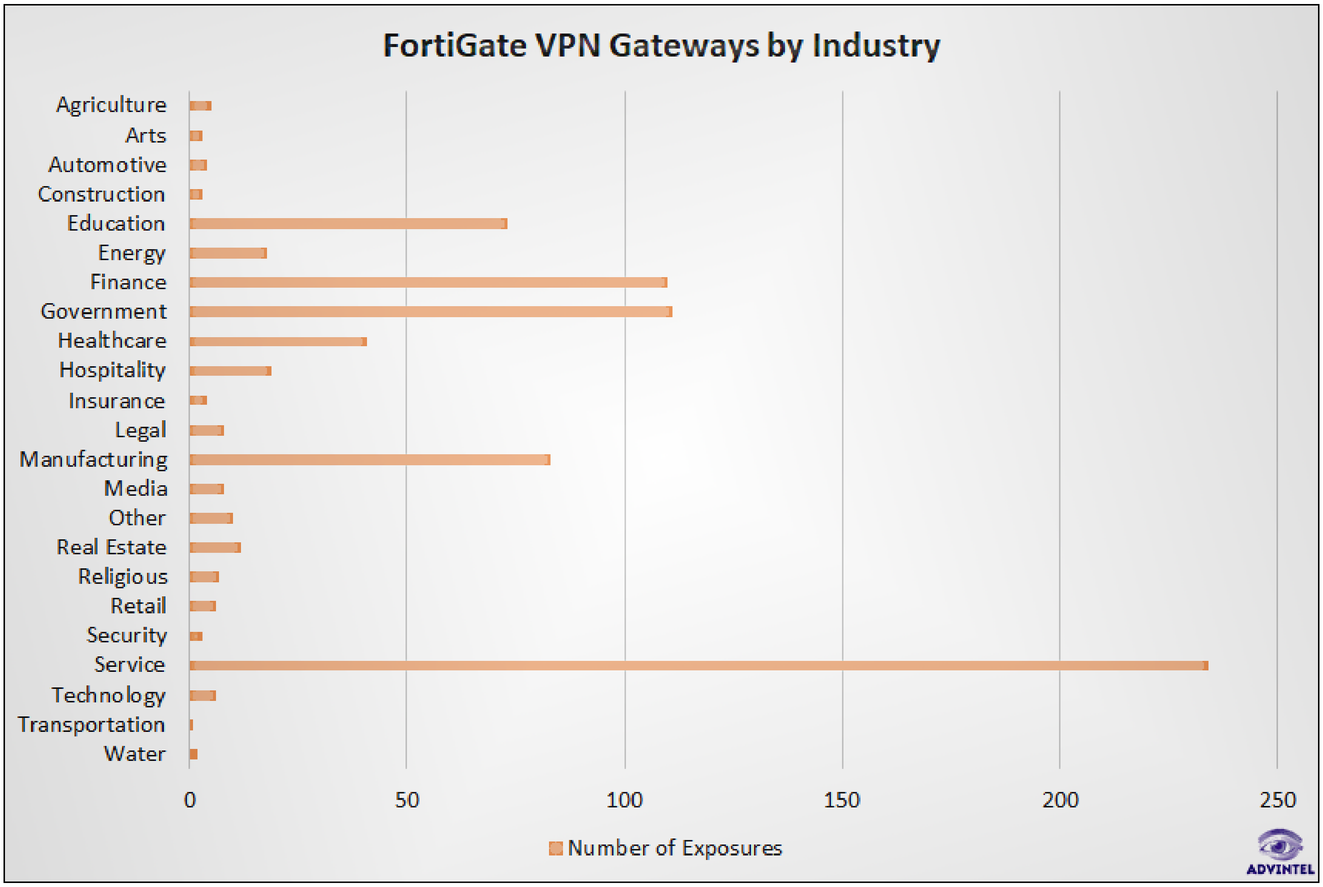
Vulnerabilities in Fortinet Fortigate VPN devices have also been disclosed recently, including CVE 2018-13379, and security researchers are reporting active exploitation [7]. Upgrading to the latest version will remove the vulnerabilities.

## Resetting Credentials

If a malicious actor previously exploited the vulnerability to collect legitimate credentials, these credentials would still be valid after patching. NSA recommends resetting credentials after a vulnerable VPN device is upgraded and before it is reconnected to the external network:

- Immediately update VPN user, administrator, and service account credentials.
- Immediately revoke and generate new VPN server keys and certificates. This may require redistributing VPN connection information to users.
- If compromise is suspected, review accounts to ensure no new accounts were created by adversaries.

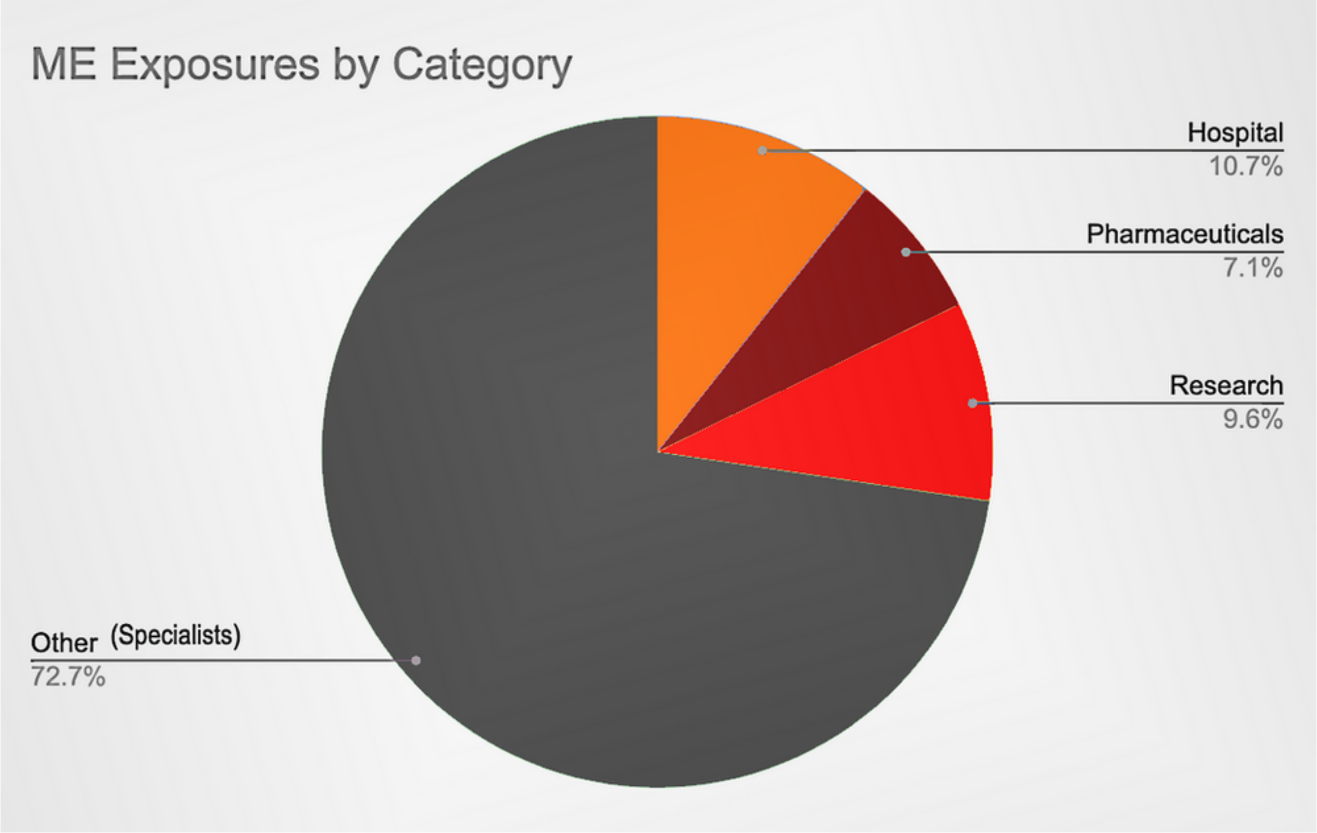
For Fortinet VPN endpoints that could be exploited by malicious actors, 41 HVTs within the healthcare sector have been identified as being at risk of exposure via **CVE-2018-13379**, **CVE-2020-12812**, and **CVE-2019-5591**. Although other sectors recorded a much higher number of HVTs with vulnerabilities, the nature of many parts of healthcare, such as managed healthcare, can amplify the damage to any of the healthcare-related HVTs.



*Data Source: AdvIntel HVT Dataset*

**Healthcare: Industry Review**

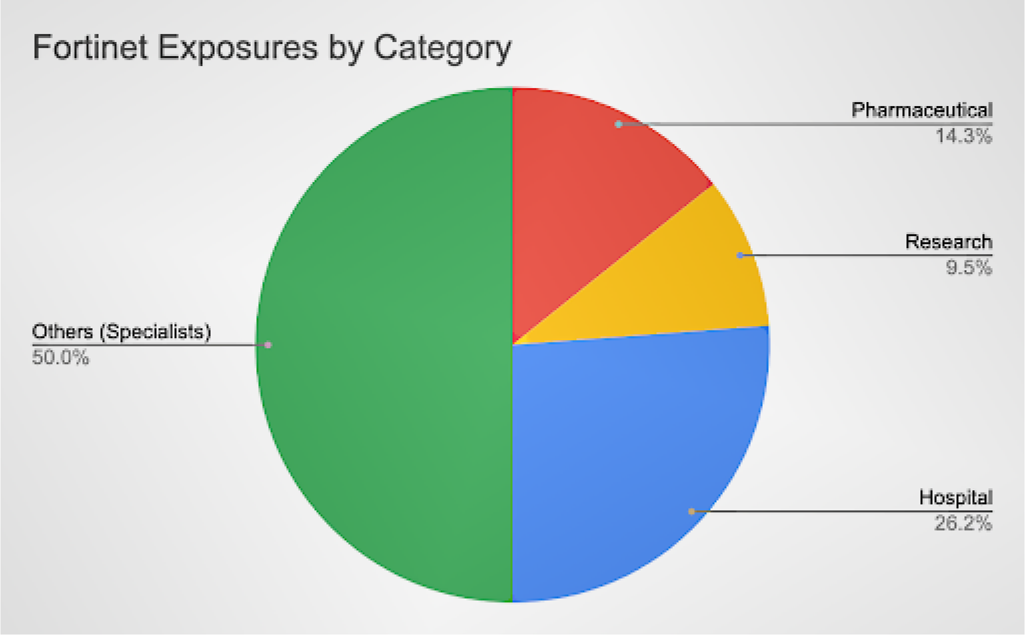
AdvIntel's **Andariel** has assessed over 2,506,718 adversarial collections related to the potentially exposed endpoints of Microsoft Exchange Servers worldwide. Statistical analysis of a sample of **8,390 High-Value Targets** that may be attacked by threat actors via ME exposure vulnerability shows that the healthcare sector has a high percentage in the dataset. Most notably, the sector has the fourth-most HVTs with potentially exposed endpoints, making up 12% of all exposures.



*The proportion between subcategories of healthcare: Data Source: AdvIntel HVT Dataset*

Of the 984 ME exposures pertaining to HVTs in the healthcare sector, many are tied to **hospitals** (10.7%), **research companies** (9.6%), and **pharmaceuticals** (7.1%). However, the proportion of data potentially exposed is likely to be unevenly distributed, since the three aforementioned categories tend to process and store much more digital information than others, such as local clinics and specialty stores.

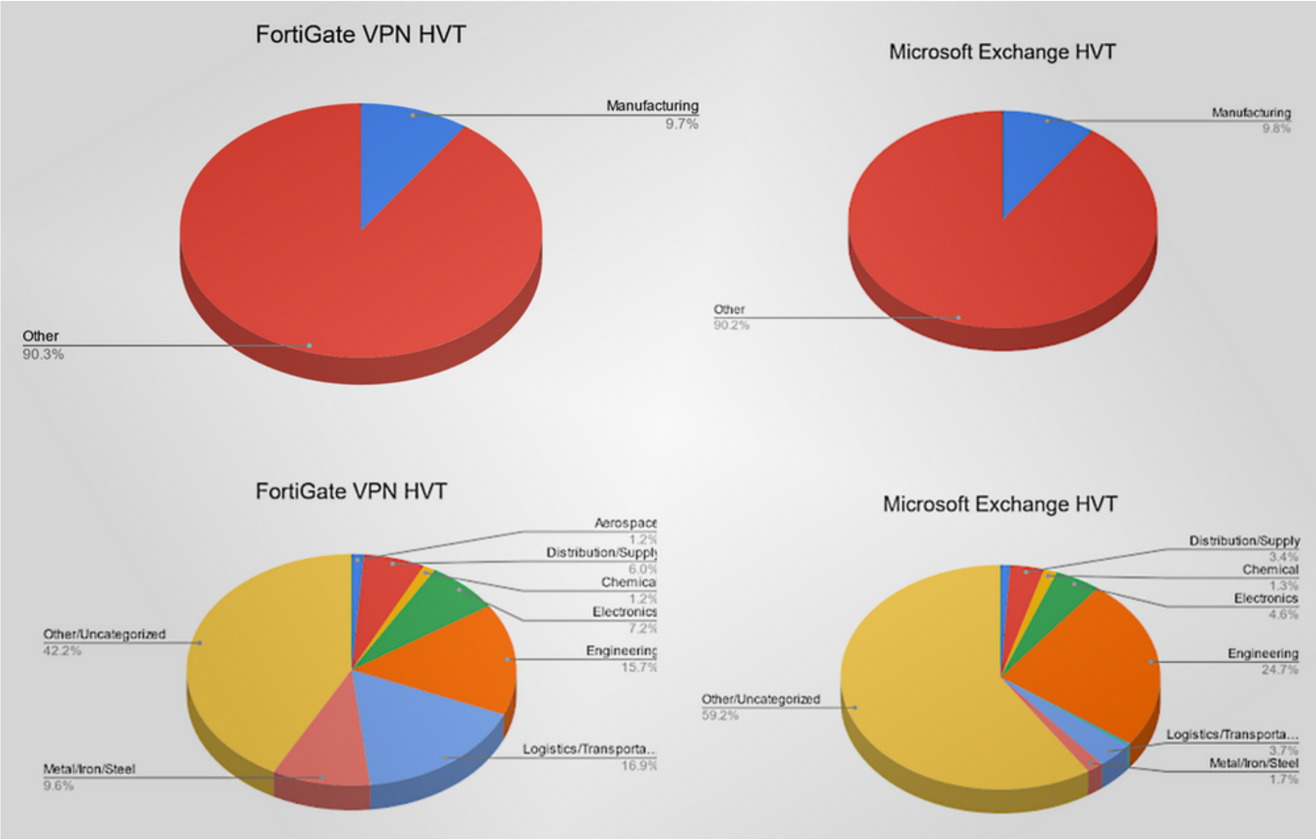
Nonetheless, other subsectors, such as medical devices companies, managed healthcare firms, and medical specialists are still vulnerable to attacks. Ransomware groups can also target these entities in order to coerce ransom payment since hospitals are prone to pay quickly in order to resume day-to-day operations.



*Data Source: AdvIntel HVT Dataset*

Of the significant Fortinet HVTs in the healthcare sector, a large proportion are related to research institutions, pharmaceuticals, and hospitals, entities that process and store a large amount of sensitive information.

### Manufacturing: Industry Review



The manufacturing sector is represented within both datasets. Manufacturing entities comprise 9.8% of potential HVT at risk of data exposure due to Microsoft Exchange vulnerabilities and 9.7% of those at risk due to Fortinet vulnerabilities. Within the sector, several subsectors are particularly present. Key examples are listed below with statistics.

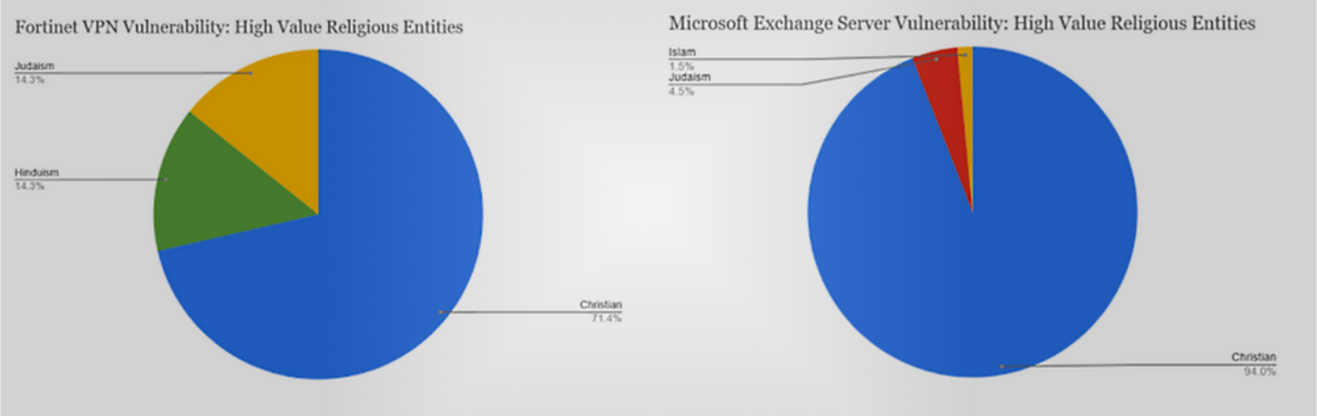
The U.S Federal Bureau of Investigation (FBI) and Cybersecurity and Infrastructure Security Administration (CISA) have warned that advanced persistent threat (APT) groups are scanning for unpatched Fortinet software in both public and private sector entities.

> *The U.S Federal Bureau of Investigation (FBI) and Cybersecurity and Infrastructure Security Administration (CISA) have warned that advanced persistent threat (APT) groups are scanning for unpatched Fortinet software in both public and private sector entities*

The manufacturing sector possesses several key traits that render it a highly exploitable target for threat actors. Manufacturing companies handle a range of highly sensitive information. Blueprints and patents for products, data on clients with long-term contracts, financial account information, and personal information on employees are all at risk to threat actors. Such information can be encrypted for ransom, exfiltrated for sale on the DarkWeb, or even be used for corporate espionage purposes.

In addition, threat actors can pose a direct risk to manufacturing infrastructure. Manufacturing is a capital-intensive enterprise that is increasingly reliant on digital technologies for production processes. If threat actors are able to seize control of a network at a manufacturing site, they can wreak havoc on production. Assembly lines may be stopped, production equipment irreparably damaged, or products ruined. Any of these outcomes would result in severe financial consequences for a firm in the form of shutdown and recovery costs, while also likely impairing the firm's reputation.

### Religious: Industry Review



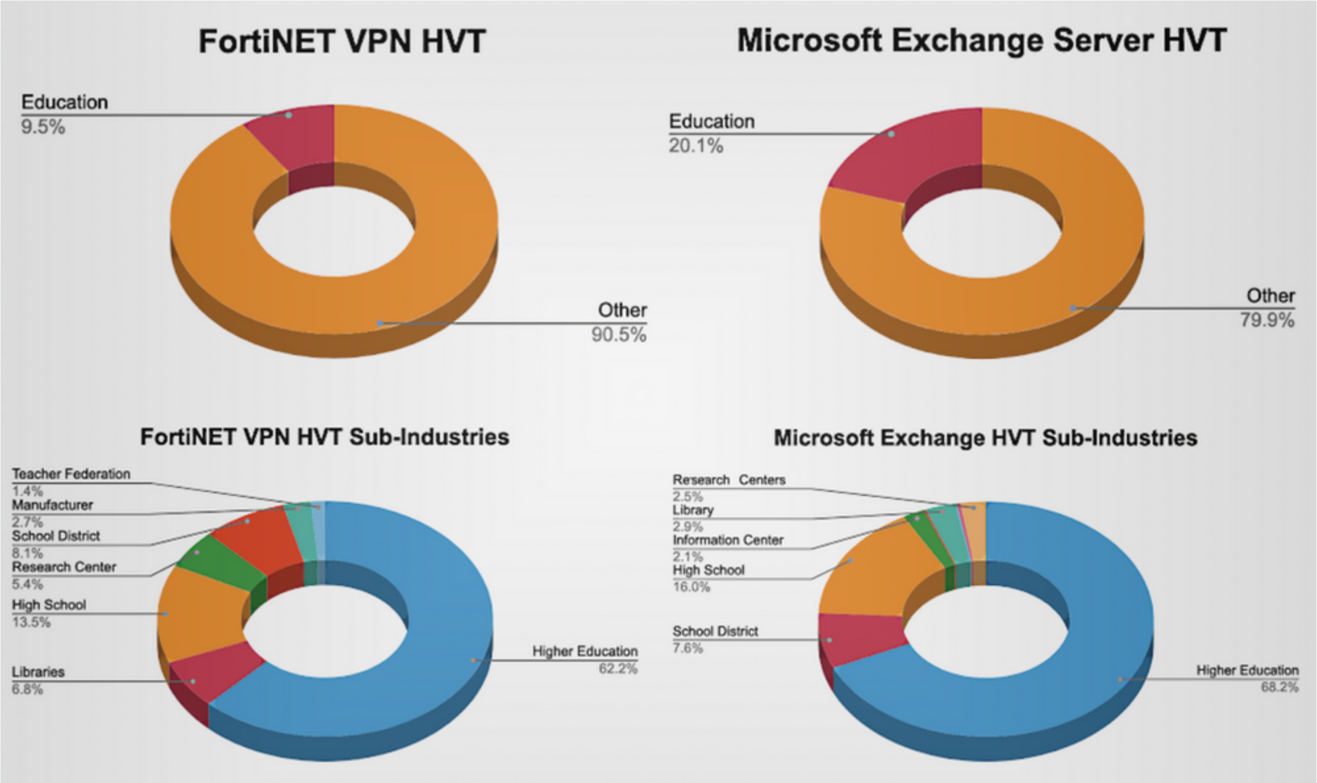
On April 02, 2021, AdvIntel analysts updated high-value target information regarding the Microsoft Exchange Server and Fortinet VPN vulnerabilities. Previously, it had been identified that 26 religious entities were considered high-value targets that contained vulnerable Microsoft Exchange Server endpoints. However, the update has increased the number to 134 high-value target religious entities. Based on AdvIntel's updated dataset, 94% of **Christian-affiliated** entities, 4.5% of **Judaism-affiliated** entities, and only 1.5% of **Islam-affiliated** entities are at risk of having potentially vulnerable endpoints.

In regards to the Fortinet VPN vulnerability, the dataset shows 71.4% of **Christian-affiliated entities**, 14.3% of **Judaism-affiliated** and **Hinduism-affiliated** entities are at risk of having potentially vulnerable gateways.

AdvIntel analysts have detected possible correlations between ransomware groups and their interests in exploiting vulnerabilities from the Microsoft Exchange Server and Fortinet VPN.

Religious entities are at risk of potentially being targeted by ransomware groups such as **REvil**, **DearCry**, **Black Kingdom**, **Hades**, and ransomware partnerships on the DarkWeb. In addition, analysis has shown **REvil**, **Clop**, and **Hades** to have a potential interest in the Fortinet VPN gateway vulnerabilities. Other known threats include advanced persistent threat groups such as **HAFNIUM** and cybercriminals on the DarkWeb.

**Education: Industry Review**

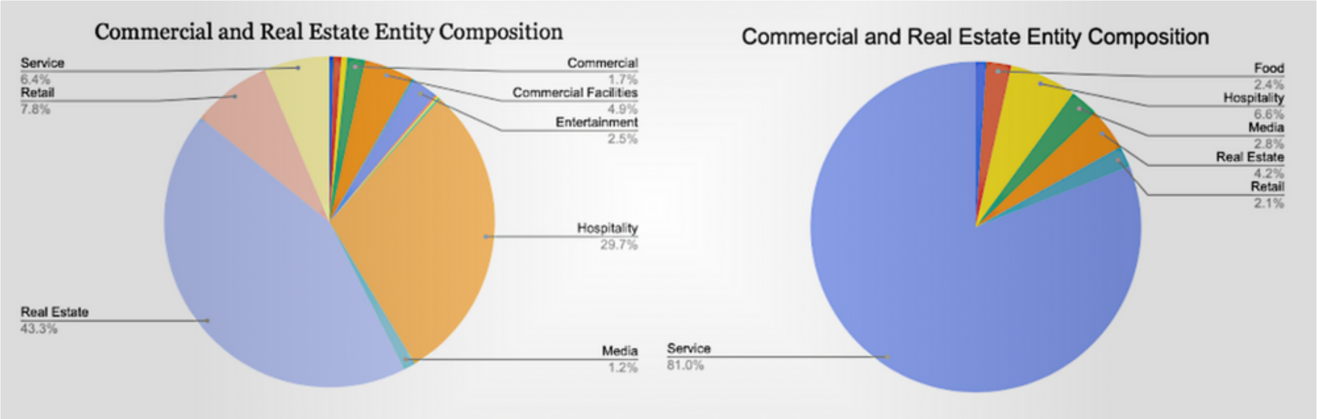


Education entities comprised 20% (1,683) of potential HVTs at risk of data exposure due to Microsoft Exchange vulnerabilities, whereas education entities comprised 9.4% (73) of the entities potentially high-value targets at risk of data exposure due to Fortinet VPN vulnerabilities.

Along with healthcare information, the education sector contains financial information of faculty, including payroll and bank account information. This data is particularly enticing to threat actors because this information can be easily exploited for large sums of money on the DarkWeb.

When a data breach has occurred in a school or university, it is not uncommon for the entity to stop its operations until IT support or federal agencies are able to resolve the cyber issue. This can result in severe financial issues as schools and universities must spend more money on resolving the issue than being proactive with IT services. It may also cost the schools money, as they may lose enrollment because of the distrust in the school or university that they can safeguard their personal information from exploitation.

### Real Estate & Commercial Facilities: Industry Review



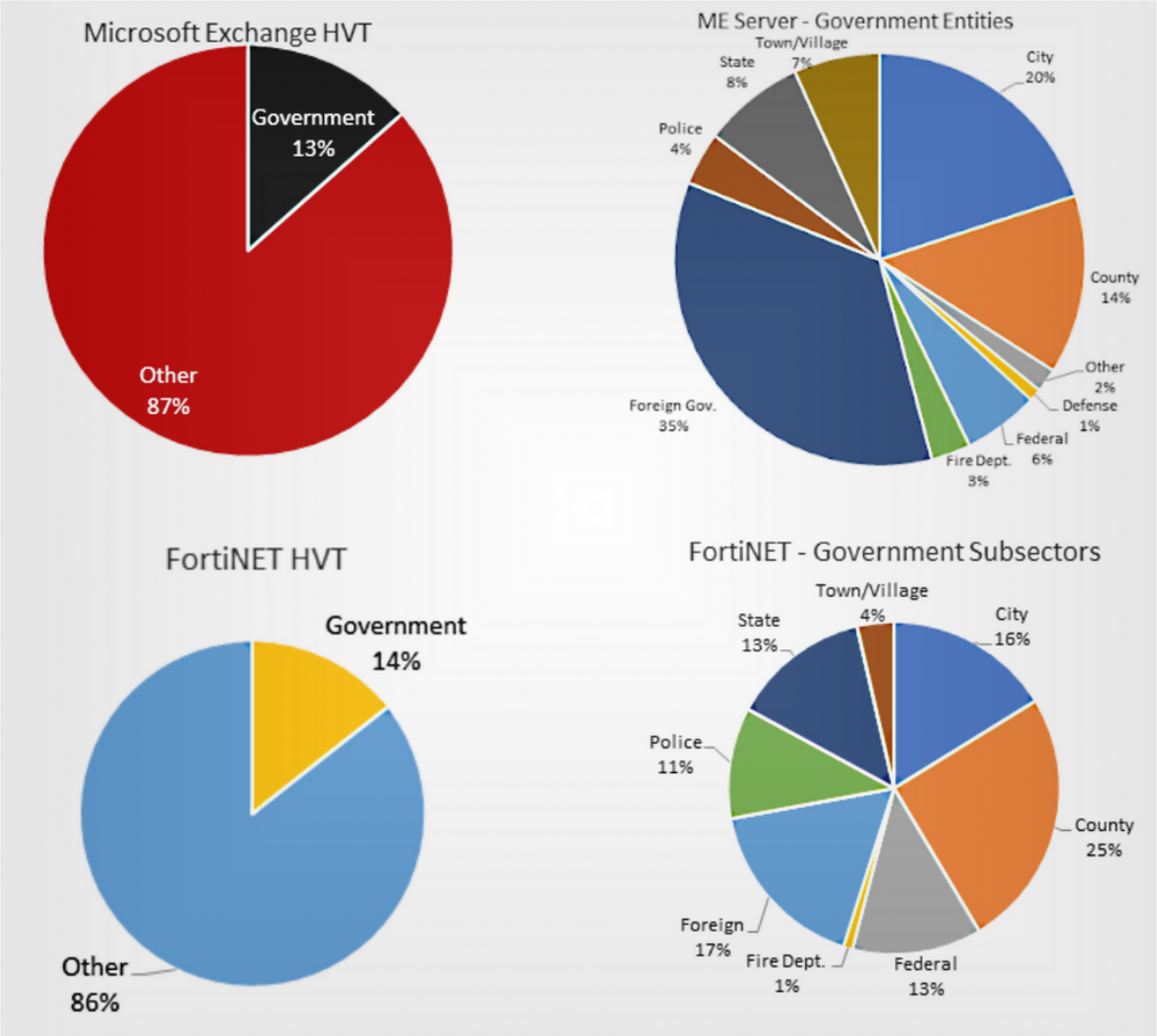
Data gathered by AdvIntel through the analysis of adversarial feeds and parsing entity data collected on Microsoft Exchange server exposure by Andariel indicate that of the total number of high-value ME server exposures detected, 10.9% are commercial or real estate entities. Comparatively, other sectors like education, government, finance make up 20.1%, 13.4%, and 19.9% respectively. Exposed commercial and real estate entities are primarily based in the United States and the United Kingdom but include entities from every continent.

Based upon the entity composition, the real estate sector is particularly vulnerable, followed by the hospitality sector. Real estate houses key financial information belonging to realty clients that can be sold on the DarkWeb and potentially used for financial fraud schemes including loan and mortgage fraud.

A close second is the hospitality sub-industry. Hospitality is unique because entities within the sector house PII and credit card information on a mass scale and continuously collect it. Card dumps operators would view an exposed endpoint from a large, high-value entity in the hospitality sub-industry as a golden opportunity to gather credit card information that can be sold on the DarkWeb or exploited by the threat actor.

**AdvIntel designated 771 total entities as high value based upon the data parsed from the Fortinet exposure. Out of the 771 total entities, entities pertaining to the commercial and real estate sector comprise 271, totaling 35.1% of HVTs.**

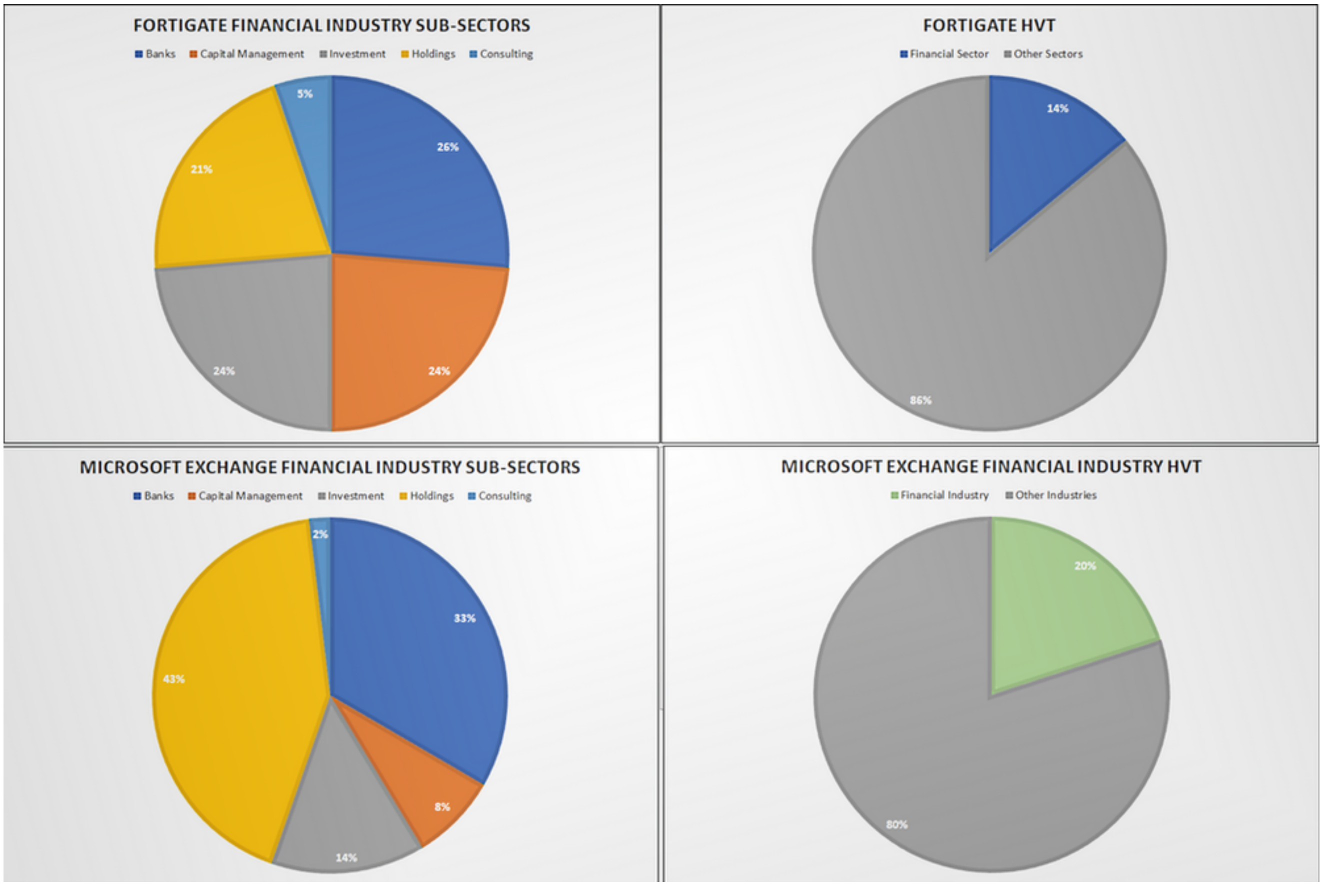
## Government & Tribal: Industry Review



While identifying government entities on the HVT dataset, AdvIntel analysts broke down the government sector into sub-sectors to gain a better insight into the entities exposed. Amongst the government entities with potential exposure points, 65% were in the **United States** while 35% were found in **other countries** around the world. In the United States, local government entities were found to have the most potentially vulnerable endpoints. **Towns or villages** make up 7%, **cities** make up 20%, and **counties** make up 14% of exposed local governments. **Local governments** are valuable targets for ransomware gangs.

Of the 771 entities, AdvIntel analysts had identified 111 of them pertaining to the government sector, which is 14% of the total entities. When broken further, the data shows that **cities** comprise 16%, **counties** comprise 25%, and **towns or villages** combined make 4%, which identifies **local government entities** as possessing potentially vulnerable endpoints at 45%. The second highest are **foreign governments** at 17%, followed by **state governments and federal governments** with both at 13% each.

### Finance: Industry Review



Finally, the financial industry entities were also majorly represented in our HVT datasets. This industry is possibly the most targeted by cybercrime gangs. AdvIntel analyzed the financial industry, which contained 110 entities from the selected data. The largest sub-sector from the FortiNet exposure belonged to banks with 26% of the total entities. **Investment organizations** and **capital management** institutions tied for second in exposures for the sub-sectors within the financial industry at 24%, while the holdings sub-sector came in third at 21%.

AdvIntel analyzed the financial industry’s 1,675 entities, which were 20% of the total exposed industries for the Microsoft Exchange exposures. The number one exposed sub-sector at 43% were holding entities, followed by banks at 33%, and investment companies were the third-largest exposed group at 14%. The two largest sub-sectors, holdings and banks, resulted in 76% of the exposed entities.

**Conclusion**

This report was focused on potential victimology for the attacks that may potentially be initiated via the exposure of both infrastructural or system CVE vulnerabilities. In the following report, AdvIntel will focus on the adversarial perspective and illustrate which groups are the most interested to perform an attack using these specific exploits or CVEs. We will demonstrate a deep dive into the DarkWeb communications and statements by the top-tier threat actor groups to illustrate how these criminal organizations are aiming to weaponize the above-listed exposures and, potentially attempt to attack the companies and organizations from the dataset analyzed in this report.

***Advanced Intelligence is an elite threat prevention firm. We provide our customers with tailored support and access to the proprietary industry-leading “Andariel” Platform to achieve unmatched visibility into botnet breaches, underground economy, and mitigate any existing or emerging threats.***