A REPORT BY unit42

THREAT TREND

THREAT LANDSCAPE REVIEW

REPORT HIGHLIGHTS

- GLOBAL MALWARE FINDINGS
- DEFENDING AGAINST KULUOZ

PALO ALTO NETWORKS | 4401 Great America Parkway | Santa Clara, CA 95054
www.paloaltonetworks.com

paloalto networks

TABLE OF **CONTENTS**

Executive Summary

It is essential that information security practitioners, from management and governance to enablement and execution, stay up to date on the trends, distribution patterns and risks presented by the ever-evolving threat landscape.

The data used for this report was derived from Palo Alto Networks® WildFire™, which automatically identifies threats from malware over a wide array of applications by executing them in a virtual environment, and observing their behavior. This data was collected from live systems in networks belonging to 2,363 different companies operating in 82 different countries. While there are currently over 4,000 organizations using WildFire to defend their networks, the data for this report was specifically collected from organizations in 10 key verticals.

- Critical Infrastructure
- Finance
- Government
- Healthcare
- High Tech
- Higher Education
- Hospitality
- Manufacturing
- Professional Services
- Retail and Wholesale

The following are key findings from this report:

- Globally, our platform detected malware delivered in over 50 distinct applications. 87% of this malware was delivered over SMTP, 11.8% through Web-Browsing (HTTP) and 1.2% in the remaining applications.
- While all verticals saw SMTP and HTTP as the primary channels for malware delivery, they varied greatly in the percentage for each. Retail and Wholesale organizations received almost 28% of malware over the web channel while Hospitality organizations received less than 2% through the same channel.
- Over 90% of unique malware samples were delivered in just one or two sessions, while a much smaller proportion was delivered in over 10,000 attacks.
- While the US is still the leading callback location across all verticals, analysis revealed a variance in callback prevalence by country based on each vertical.
- One malware family, known as Kuluoz or Asprox, was responsible for approximately 80% of all attack sessions recorded in the month of October. This malware sends copies of itself over e-mail quickly and to users all around the world and then attempts to download additional malware, impacting 1,933 different organizations.

Introduction

The Palo Alto Networks WildFire platform analyzes over half a million files every day to automatically identify threats and quickly prevent organizations from being compromised. This system is a key component of our Threat Intelligence Cloud that helps ensure our platform can defend against the latest attacks. The purpose of this paper is to examine a subset of this data and identify how organizations in different industries are targeted by malware.

The type of analysis in this report is available through our Enterprise Risk Report, which helps organizations determine how their network compares to those of their industry peers with regard to malware attacks.

When a potentially malicious file passes through one of our Next Generation Firewalls, it can be passed to WildFire for analysis where it is executed in a sandbox environment. Within that environment, WildFire tracks the behaviors exhibited by the file to determine whether or not it is malicious and then returns a verdict to the originating firewall, which submitted the sample. Each submission of a file is tracked by our system as a "session" and each unique file is tracked as a "sample." One sample may be contained in a single session or many sessions depending on how it was distributed. The sample can be any one of the following file types and delivered through any of over 1,924 applications detected by our platform:

- Windows Executables
- Microsoft Office Documents
- RTF (Rich Text Format) Files
- Java JAR Files
- Android APKs
- Adobe Flash Applets
- PDF (Portable Document Format) Files
- JavaScript Files

For the production of this paper our team examined 6.1 million malicious sessions logged during the month of October 2014. Specifically, we examined sessions generated by 2,363 select enterprise customers across 82 countries and 10 key industries. This data only includes sessions where WildFire determined the file delivered was malware.

These 10 industries are described as follows:

- **Healthcare:** hospitals, clinics, and organizations associated with health and human services
- **Finance:** banks, insurance, credit union, and financial advisory companies
- **High Tech:** organizations focused on software development or design of new hardware
- **Hospitality:** hotels, lodging, entertainment, and non governmental community organizations
- **Manufacturing:** organizations focused on producing and fabricating machinery and materials

- **Critical Infrastructure:** energy, utilities and power generation and distribution organizations, including SCADA
- **Higher Education:** institutions of learning above the secondary school level
- **Government:** organizations from municipal up to national administrative departments
- **Retail and Wholesale:** wholesale, retail, and end client distributors of manufactured goods
- **Professional Services:** organizations providing legal and business support functions

In the following sections we compare how each of these industries was targeted based on the types of applications and files used in each attack. Additionally, we have included a section describing findings specific to one malware family, known as Kuluoz, which has been highly active in 2014.

Global Findings

In the 6.1 million malicious sessions detected by WildFire included in this data set, we identified just 360,409 unique malware samples. On average each unique sample was delivered in approximately 17 sessions, but looking closer at the data reveals a very wide distribution.

As Figure 1 shows, over 90% of the samples were delivered in two or fewer sessions, with less than one percent of samples delivered in 1,000 or more sessions.

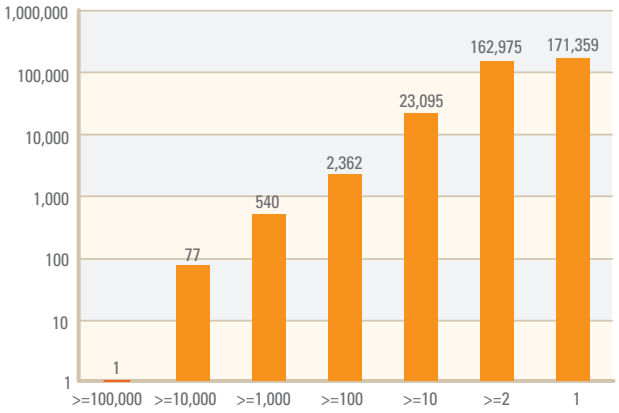


Figure 1: Total sessions for each unique sample

The most-distributed sample in the data was included in 125,288 individual sessions to 186 different companies across all 10 industries included in this report. The malware in question is a downloader Trojan that downloads and installs additional malware on the system to conduct click fraud.

While this malware was the most popular, it did not target all industries in the same way. Higher Education and High Tech organizations accounted for over 80% of the sessions tracked for this sample. These verticals have generally displayed a higher number of malware sessions than the others. In fact, Higher Education, High Tech, and Healthcare accounted for over half of the malicious sessions identified in October. On average, Higher Education organizations saw the highest number of malicious sessions per day, as shown in Figure 2.

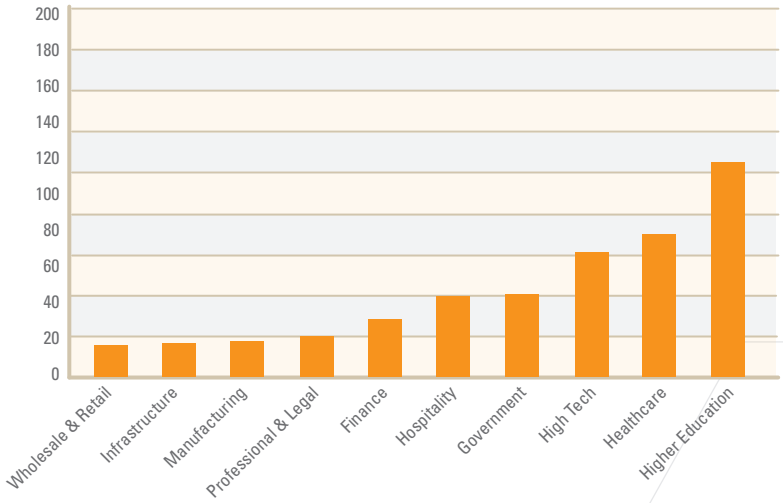


Figure 2: Average (mean) number of malicious sessions per day for a single customer in each vertical.

While WildFire can accept files from any of the applications our platform identifies, the majority of malware is delivered over two channels: SMTP (Simple Mail Transfer Protocol) and Web-Browsing. SMTP is the protocol used to transmit e-mails from one location to another, and Web-Browsing is our broad category to describe web (HTTP) traffic that we haven't categorized into a more specific category (e.g. Facebook or Gmail). In total, we identified malware transmitted through over 50 applications in the selected data, but the majority of these applications accounted for only a small percentage of the attacks, as shown in Figure 3.

Similarly, the majority of the malware detected in the sample data was delivered in the form of a Windows executable (either an EXE or DLL file), with a much smaller percentage (0.8%) delivered as a Microsoft Office document and the remaining file types making up just 0.1%.

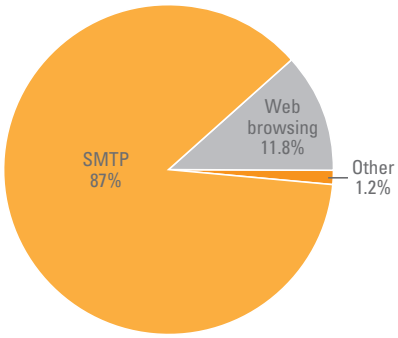


Figure 3: Proportion of sessions delivering malware for each App.

In the process of determining whether or not a file is malware, WildFire executes each sample in a live sandbox environment and monitors for Command and Control (C2) activity as well as other malicious activity. Using this data we can identify IP addresses contacted by each sample and based on geo-location data we can determine in which countries those IP addresses reside.

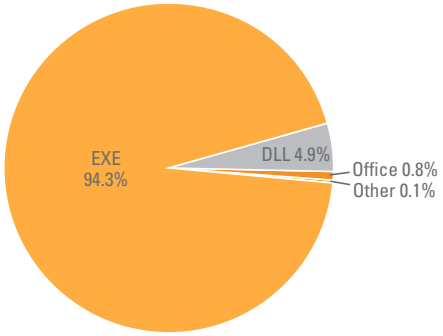


Figure 4: Proportion of sessions delivering malware of each file type.

Based on this data we found that the United States, Italy, and Germany were the top three countries contacted based on the total number of connections made by analyzed samples. The heatmap below shows the relative distribution of potential C2 activity from the 360,409 samples included in this analysis.

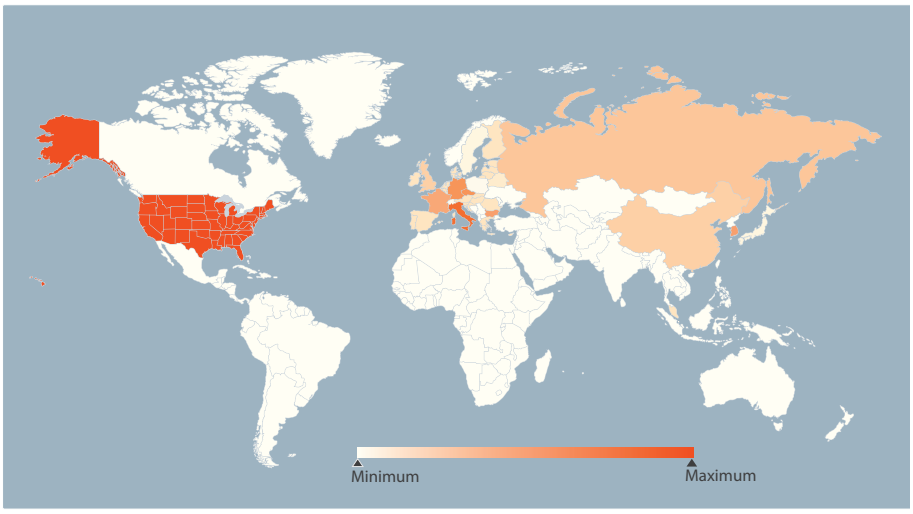


Figure 5: Possible callback locations used by malware samples

Aggregated data from the 2,363 organizations included in this report is helpful in identifying broad trends that cross verticals, but not every vertical exhibits the same trends. Organizations have different threat profiles and user environments and while some attacks may target all of them, others are the subject of direct targeting. The following sections compare the 10 verticals to the aggregate data to show how each one differs from the others.

Critical Infrastructure

The data contained in this section is from energy companies, utilities and power generation and distribution organizations.

Figure 6: Types of malicious files detected in Critical Infrastructure organizations.

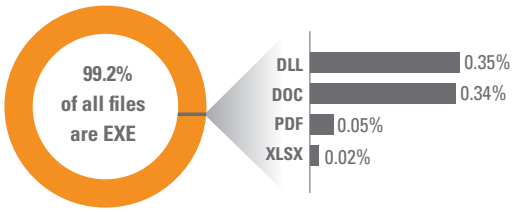


Figure 7: Types of files detected in Critical Infrastructure organizations compared to the whole.

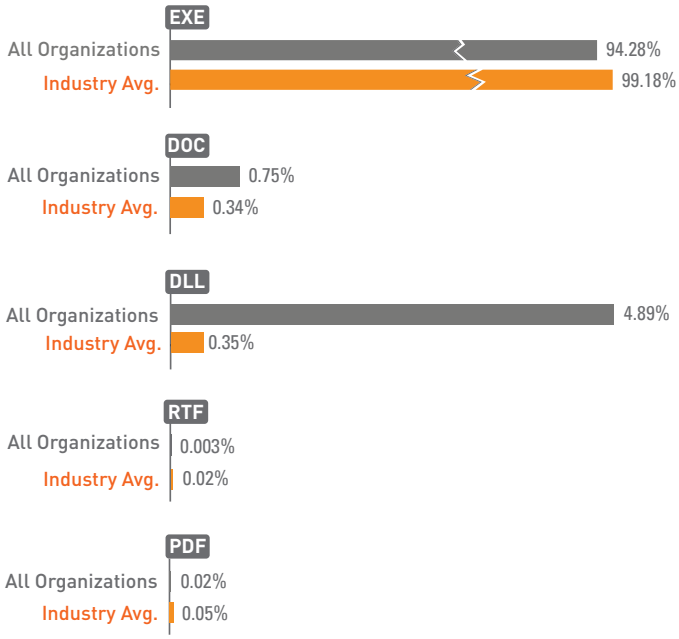
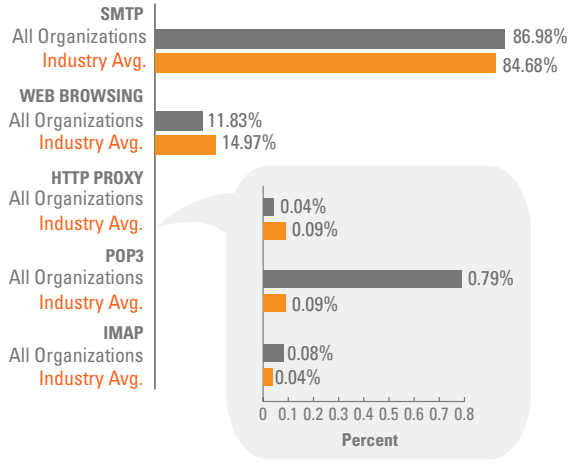


Figure 8: Applications used to deliver malware to Critical Infrastructure organizations.



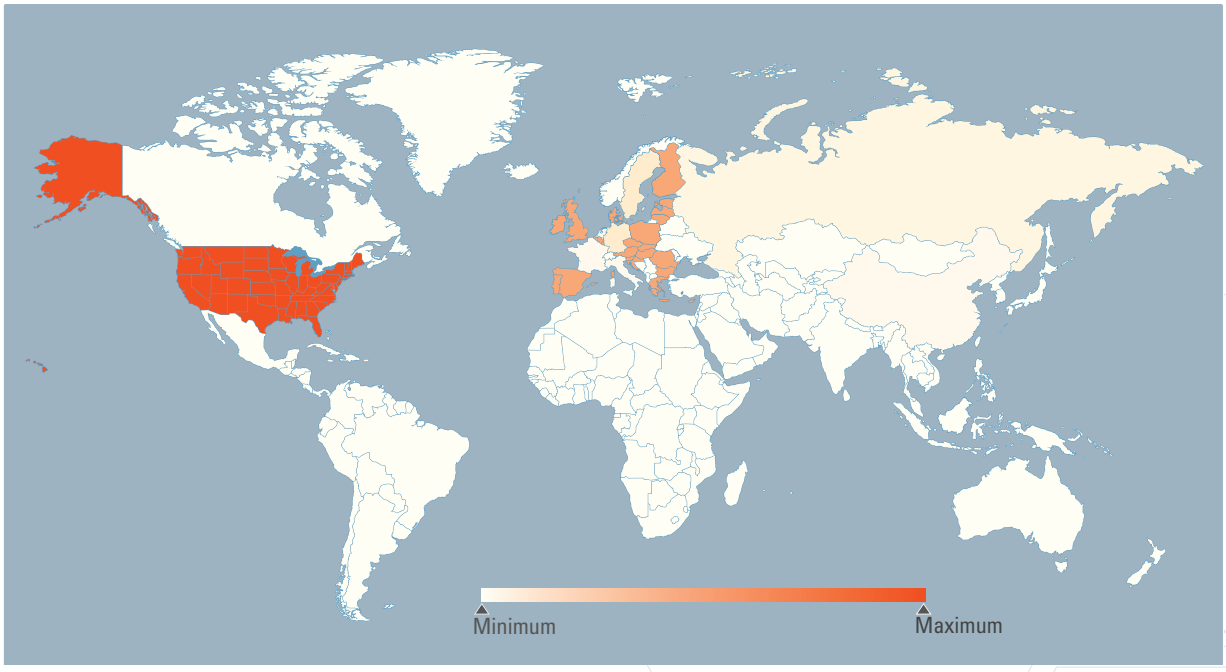


Figure 9: Possible callback locations used by malware samples delivered to Critical Infrastructure organizations.

Finance

The data contained in this section is from banks, insurance companies, credit unions, and financial advisory companies.

Figure 10: Types of malicious files detected in Finance companies.

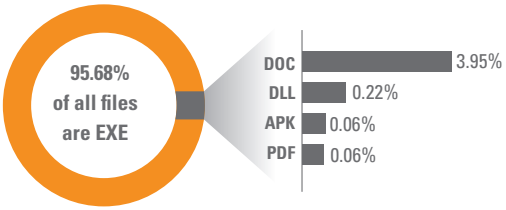


Figure 11: Types of files detected in Finance companies compared to the whole.

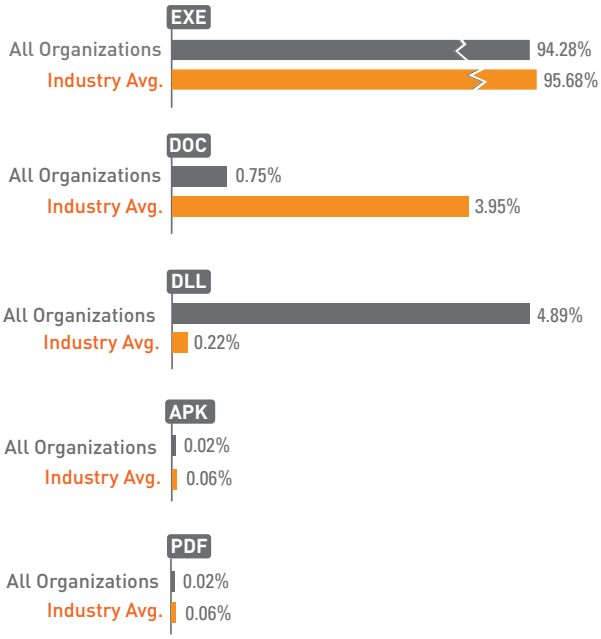
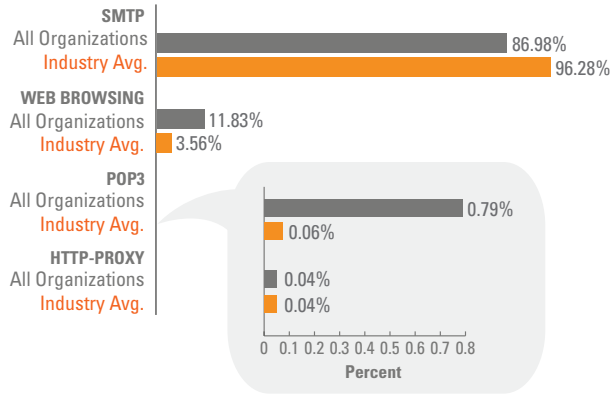


Figure 12: Applications used to deliver malware to Finance companies.



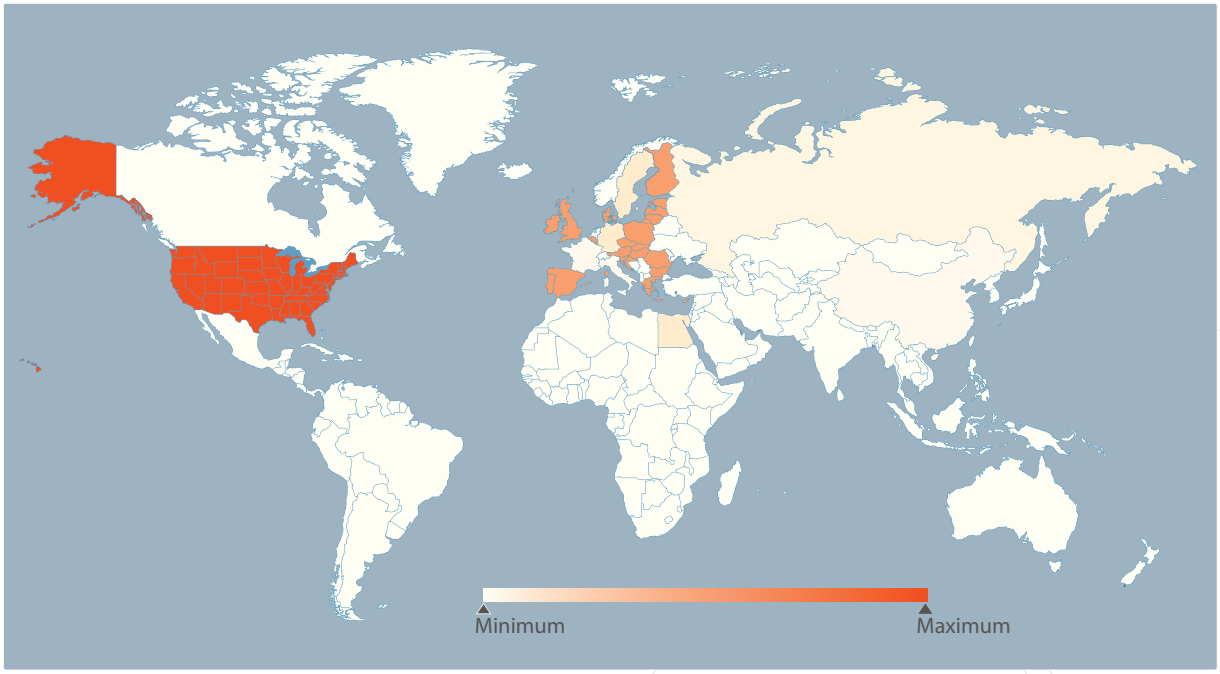


Figure 13: Possible callback locations used by malware samples delivered to Finance companies.

Government

The data contained in this section is from organizations from municipal up to national administrative departments.

Figure 14: Types of malicious files detected in Government organizations.

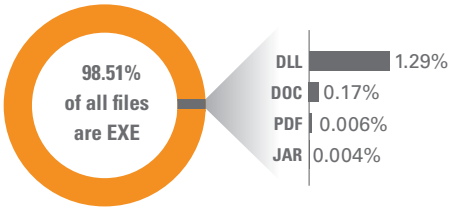


Figure 15: Types of files detected in Government organizations compared to the whole.

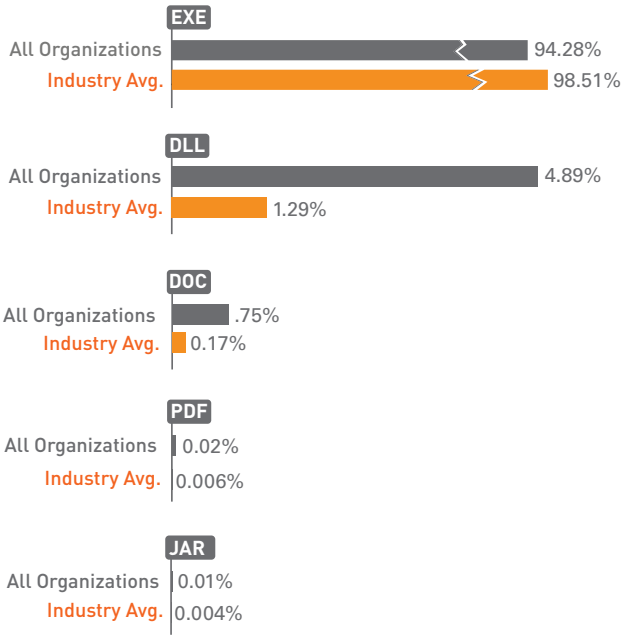
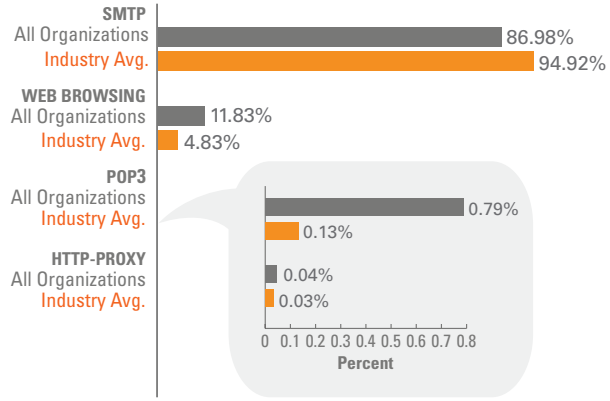


Figure 16: Applications used to deliver malware to Government organizations.



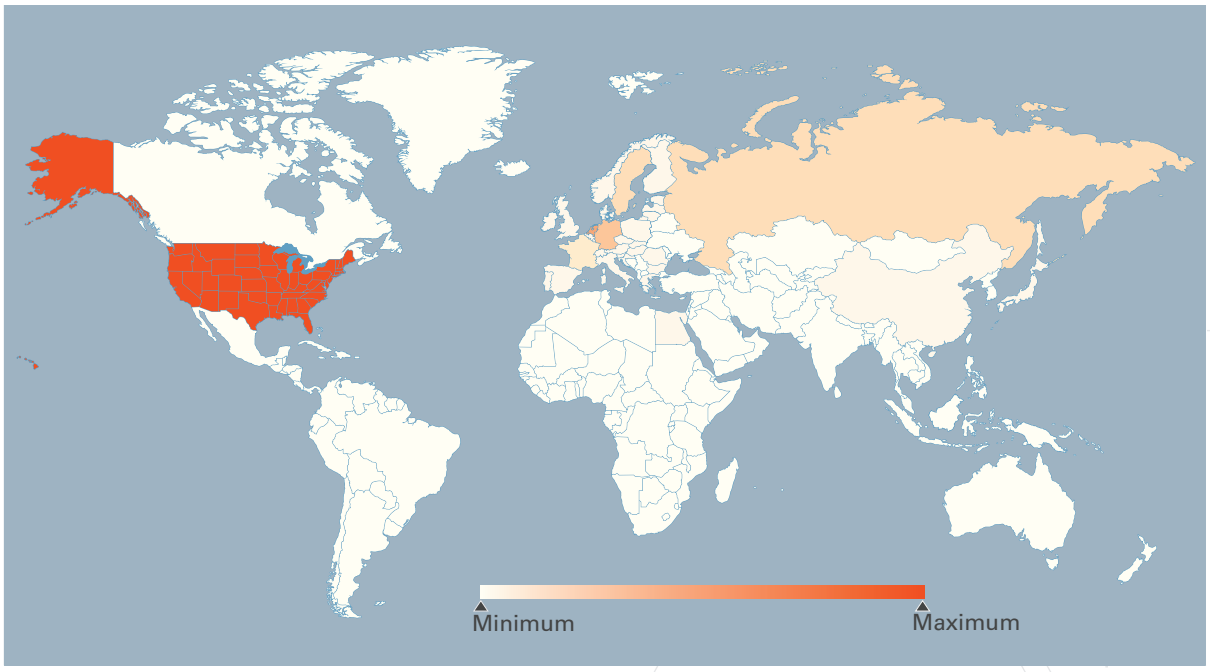


Figure 17: Possible callback locations used by malware samples delivered to Government organizations.

Healthcare

The data contained in this section is from hospitals, clinics, and organizations associated with health and human services.

Figure 18: Types of malicious files detected in Healthcare organizations.

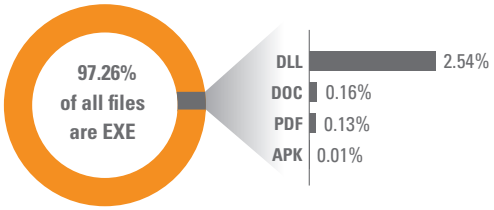


Figure 19: Types of files detected in Healthcare organizations compared to the whole.

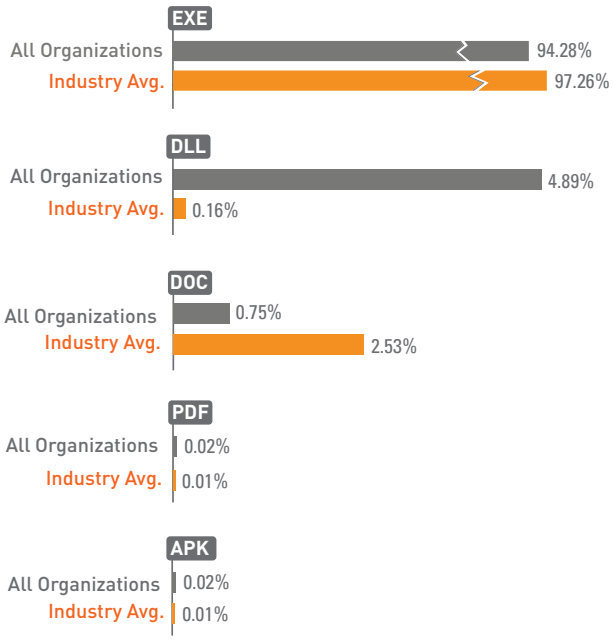
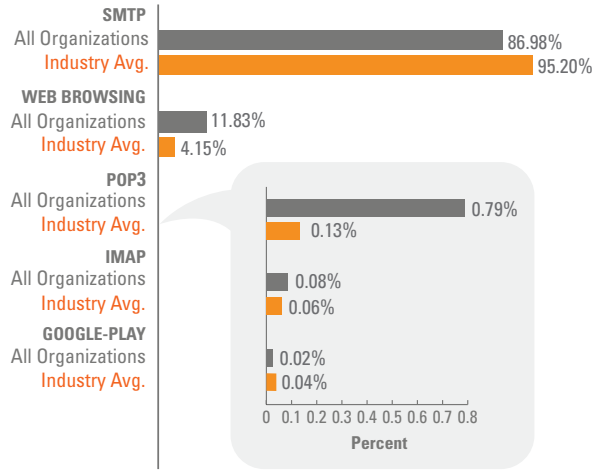


Figure 20: Applications used to deliver malware to Healthcare organizations.



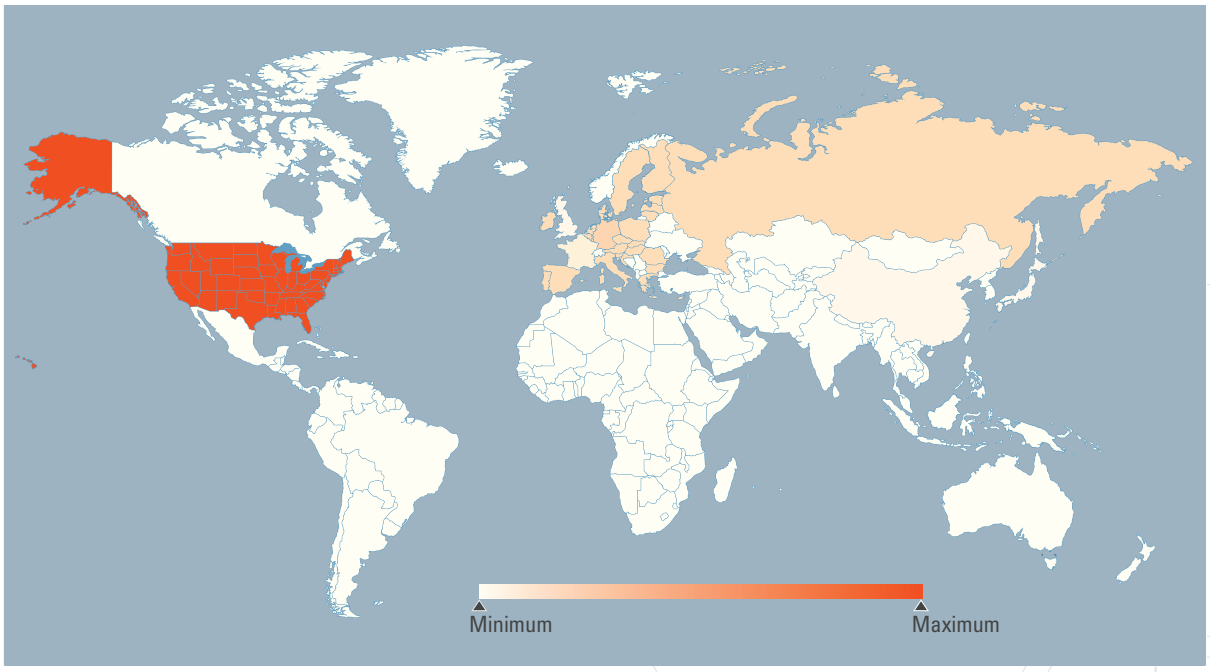


Figure 21: Possible callback locations used by malware samples delivered to Healthcare organizations.

High Tech

The data contained in this section is from companies focused on software development or design of new hardware.

Figure 22: Types of malicious files detected in High Tech companies.

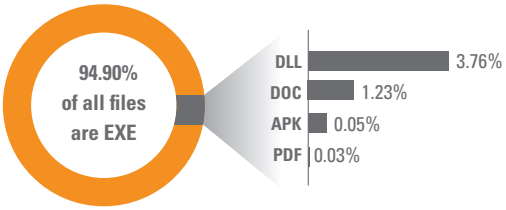


Figure 23: Types of files detected in High Tech companies compared to the whole.

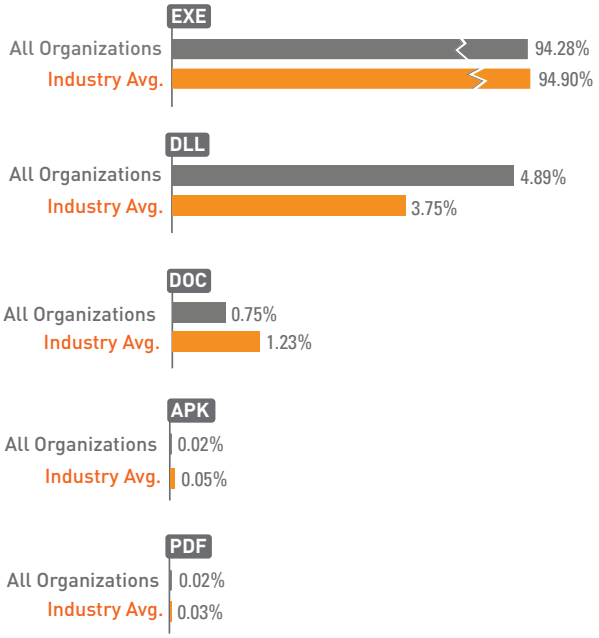
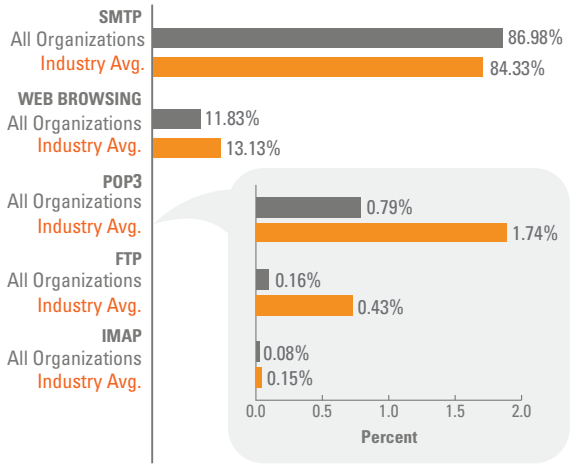


Figure 24: Applications used to deliver malware to High Tech companies.



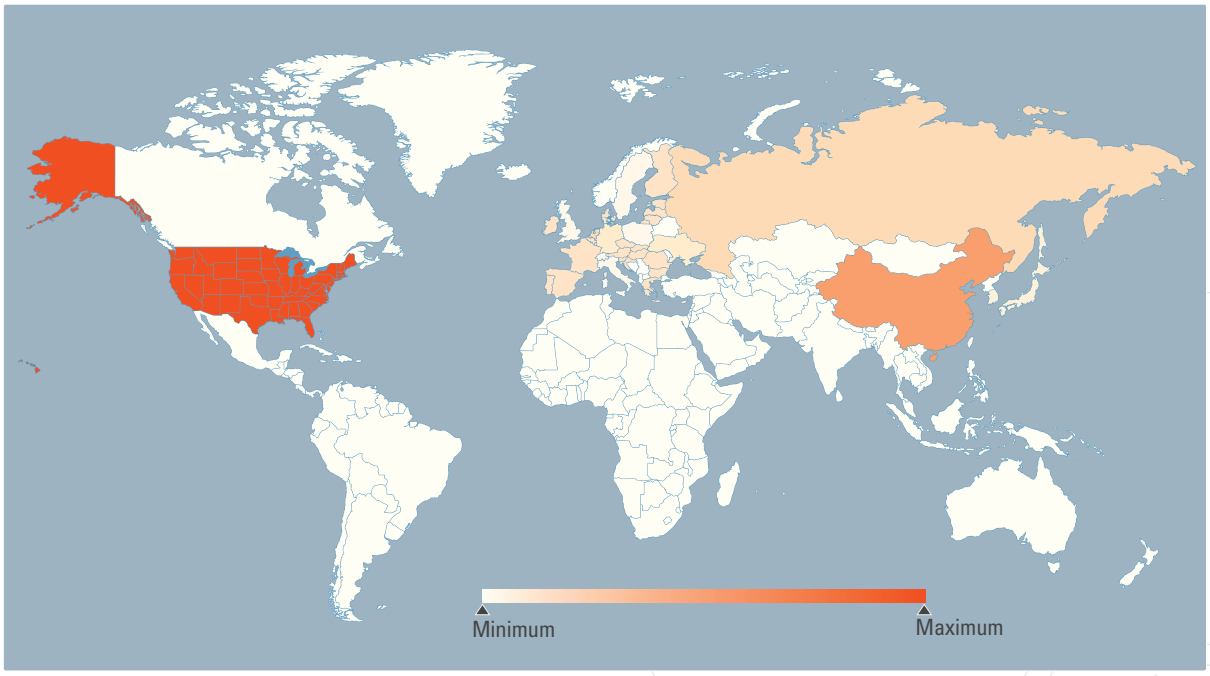


Figure 25: Possible callback locations used by malware samples delivered to High Tech companies.

Higher Education

The data contained in this section is from institutions of learning above the secondary school level.

Figure 26: Types of malicious files detected in Higher Education institutions.

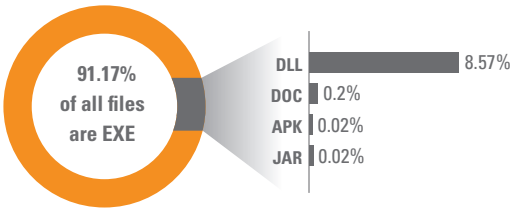


Figure 27: Types of files detected in Higher Education institutions compared to the whole.

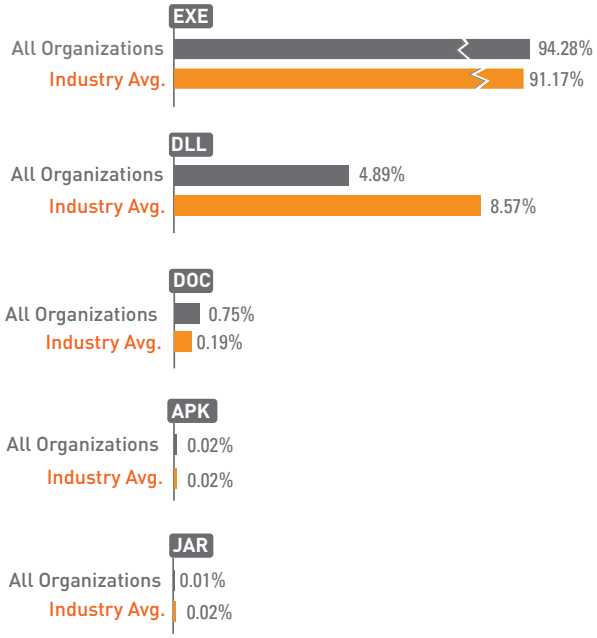
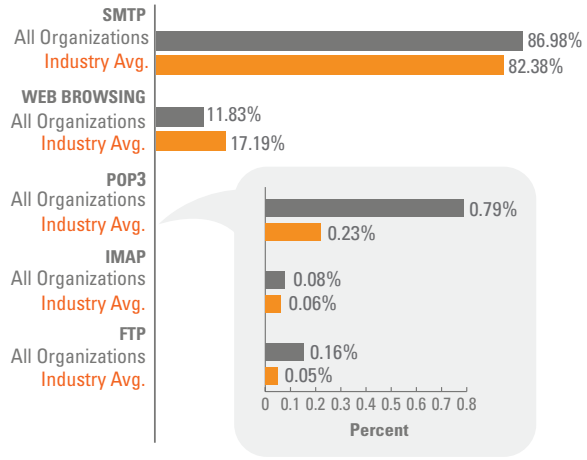


Figure 28: Applications used to deliver malware to Higher Education institutions.



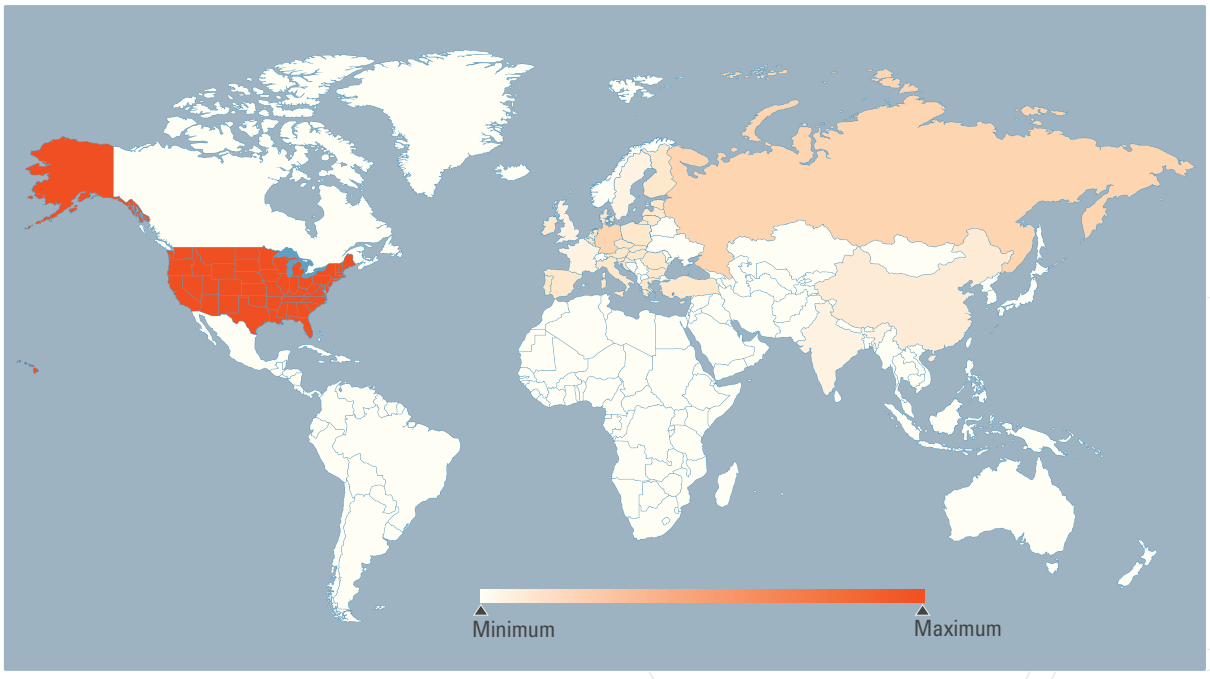


Figure 29: Possible callback locations used by malware samples delivered to Higher Education institutions.

Hospitality

The data contained in this section is from hotels, lodging, entertainment, and non-governmental community organizations.

Figure 30: Types of malicious files detected in Hospitality organizations.

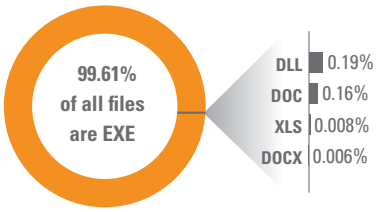


Figure 31: Types of files detected in Hospitality organizations compared to the whole.

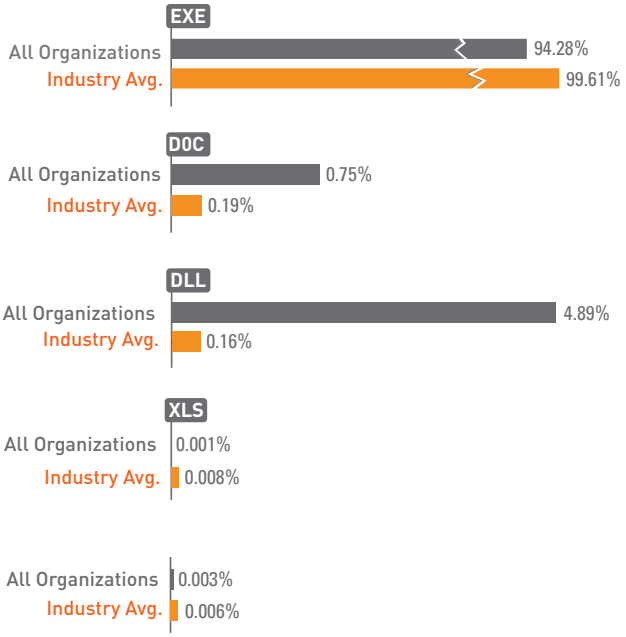
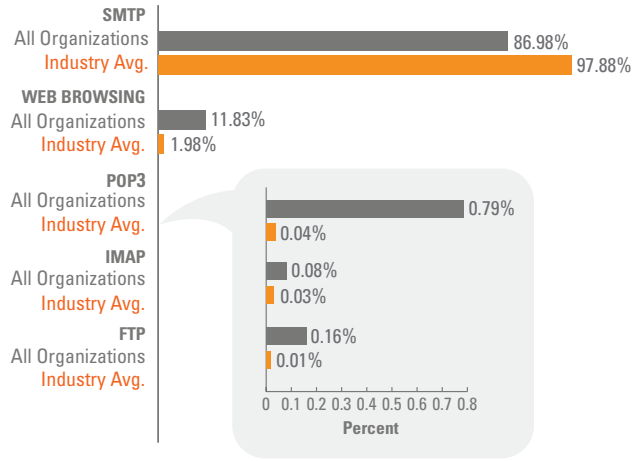


Figure 32: Applications used to deliver malware to Hospitality organizations.



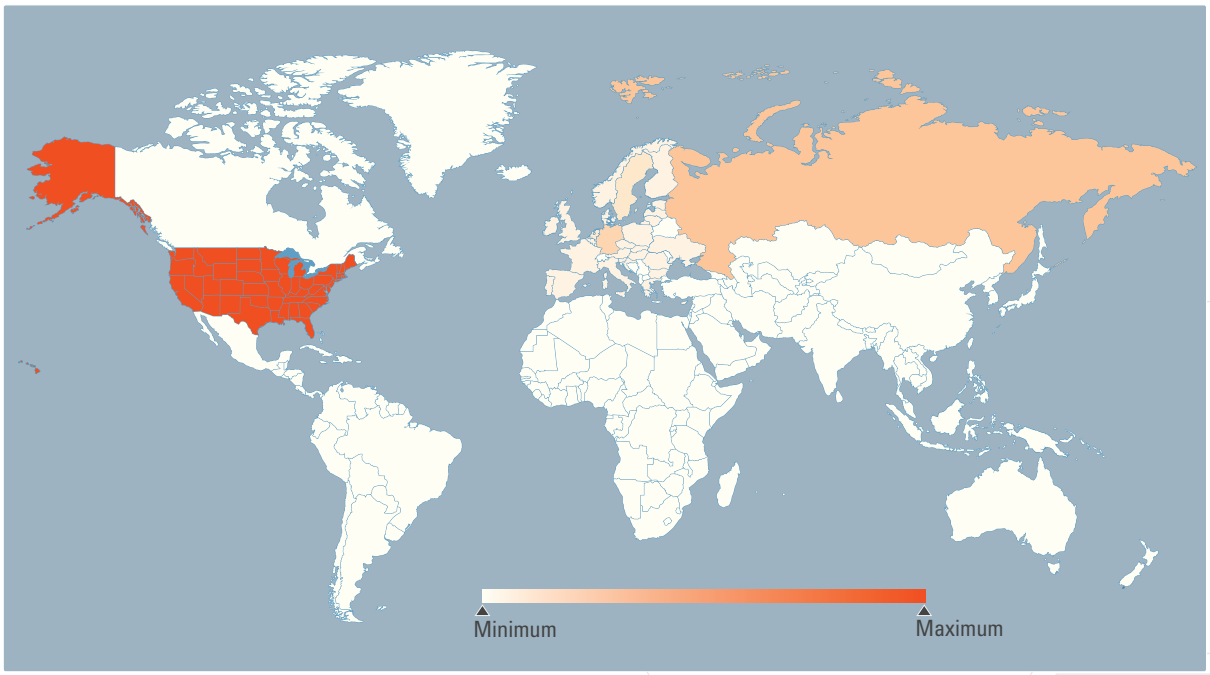


Figure 33: Possible callback locations used by malware samples delivered to Hospitality organizations.

Manufacturing

The data contained in this section is from companies focused on producing and fabricating machinery and materials.

Figure 34: Types of malicious files detected in Manufacturing companies.

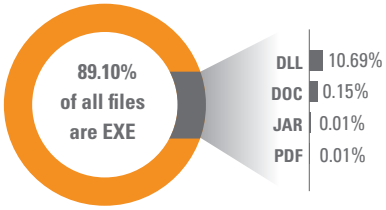


Figure 35: Types of files detected in Manufacturing companies compared to the whole.

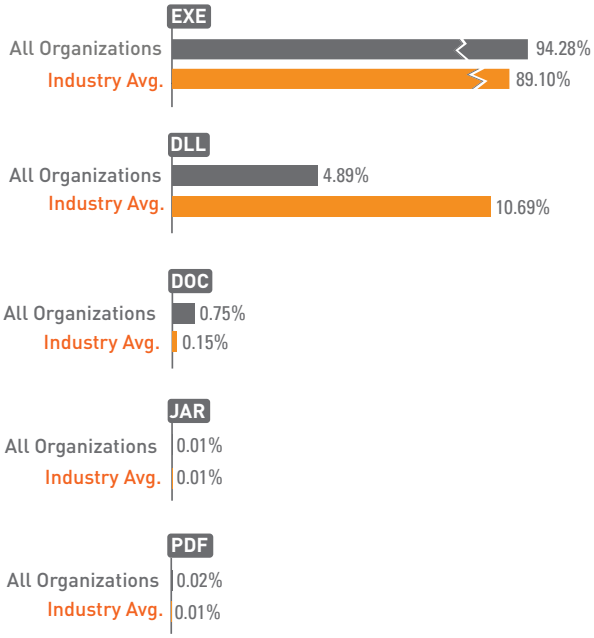
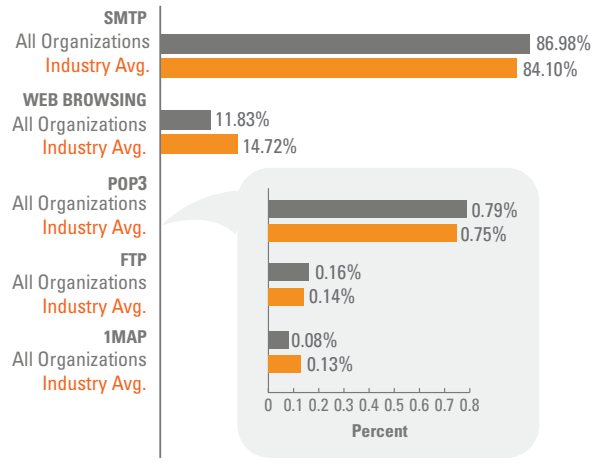


Figure 36: Applications used to deliver malware to Manufacturing companies.



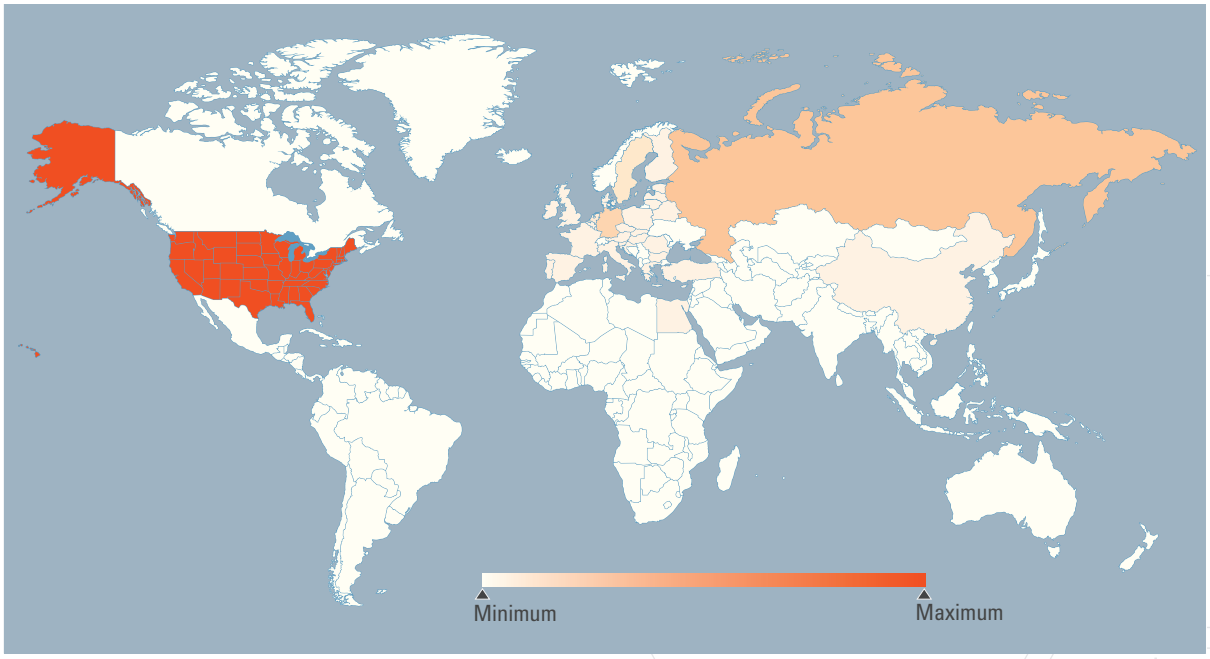


Figure 37: Possible callback locations used by malware samples delivered to Manufacturing companies.

Professional Services

The data contained in this section is from organizations providing legal and business support functions.

Figure 38: Types of malicious files detected in Professional Services organizations.

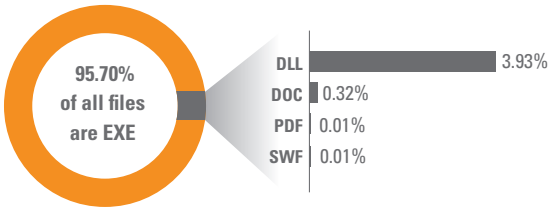


Figure 39: Types of files detected in Professional Services organizations compared to the whole.

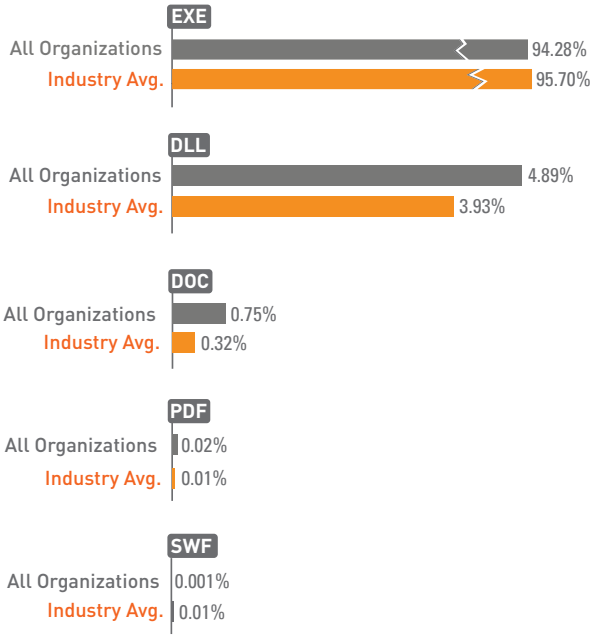
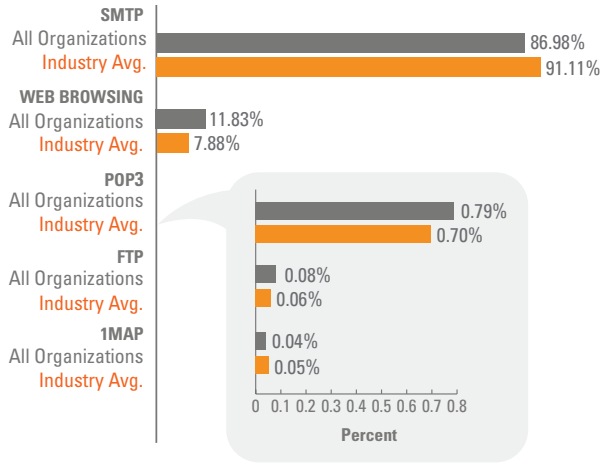


Figure 40: Applications used to deliver malware to Professional Services organizations.



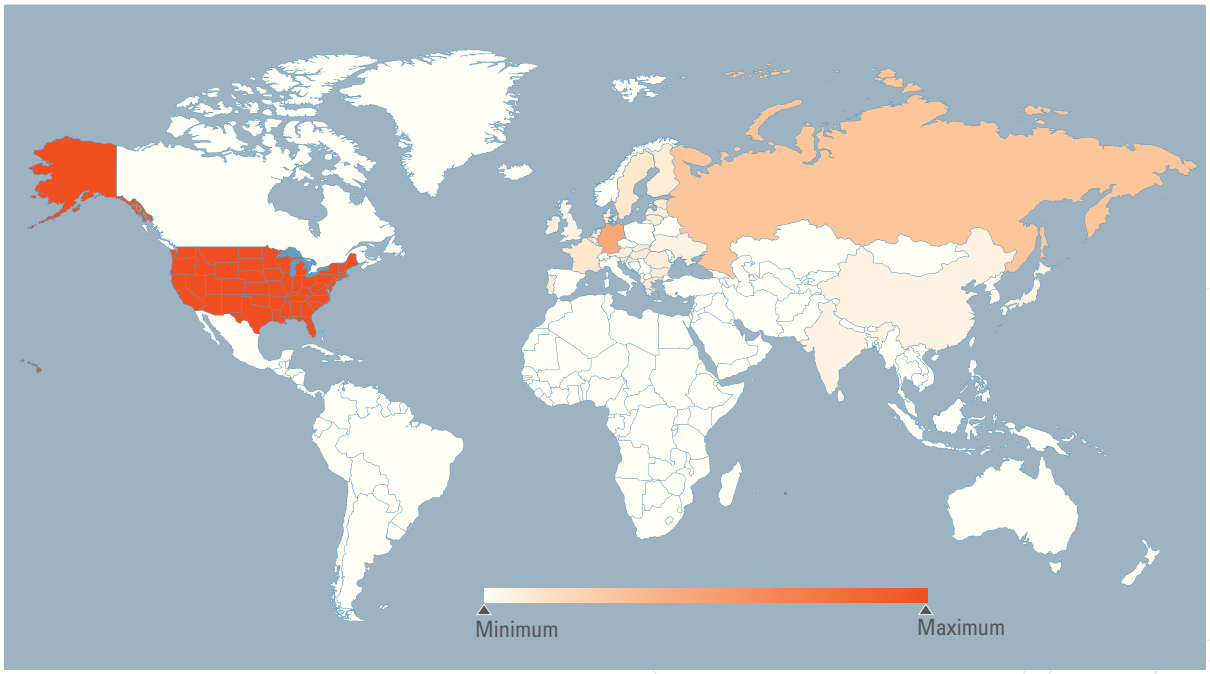


Figure 41: Possible callback locations used by malware samples delivered to Professional Services organizations.

Retail and Wholesale

The data contained in this section is from wholesale, retail, and end client distributors of manufactured goods.

Figure 42: Types of malicious files detected in Retail and Wholesale companies.

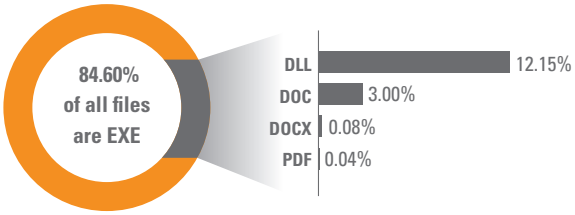


Figure 43: Types of files detected in Retail and Wholesale companies compared to the whole.

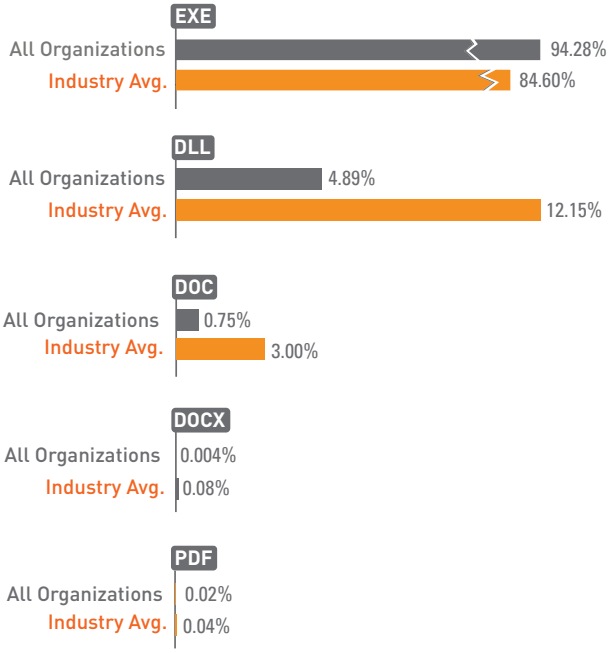
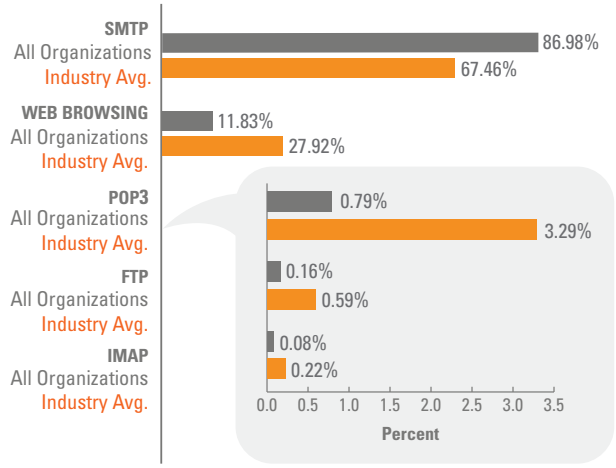


Figure 44: Applications used to deliver malware to Retail and Wholesale companies.



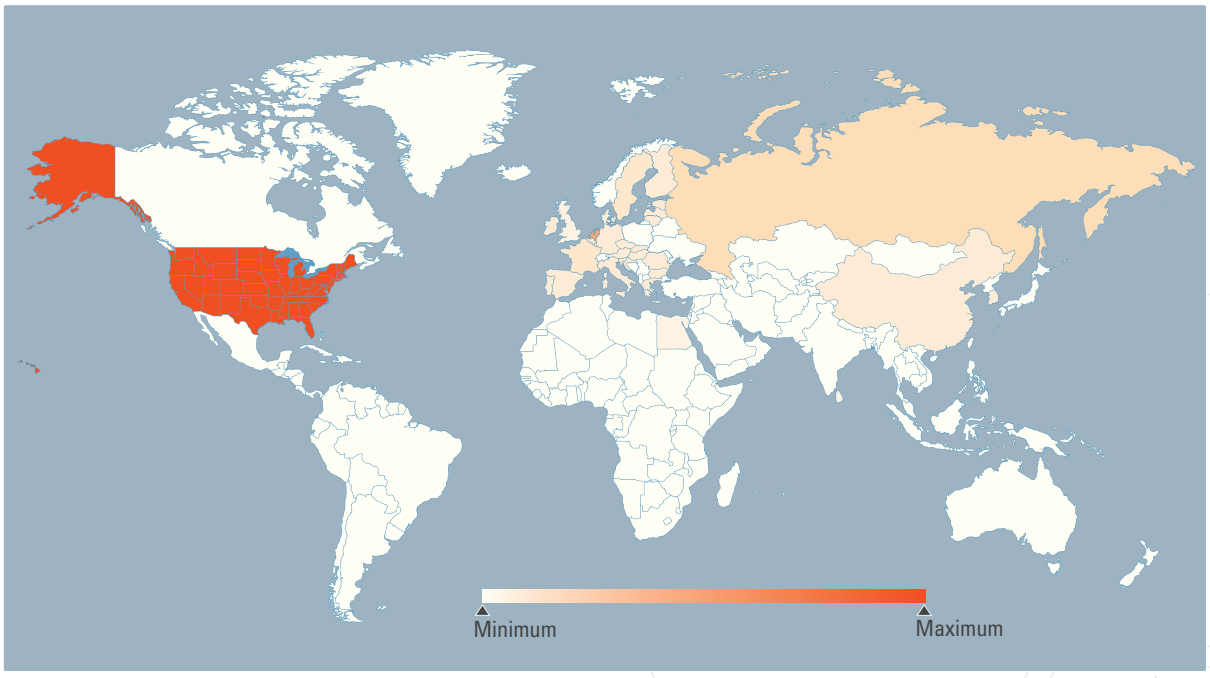


Figure 45: Possible callback locations used by malware samples delivered to Retail and Wholesale companies.

Threat Highlight: Kuluoz

One particular malware family, Kuluoz (also known as Asprox), stood out as exceptionally prevalent in the sample data. This single family accounts for 4.9 million malicious sessions recorded during the month of October 2014, with 1,933 companies across all 10 industries impacted. WildFire identified a total of 268,084 unique samples determined to be Kuluoz, 82.4% of which had not been collected by VirusTotal at the time of analysis.

KULUOZ STATISTICS	
% of Companies Impacted	81.8
% of Malicious Sessions	80.0
% of Unique Malware	74.4

The first version of Asprox appeared in 2007, and it was given its name by researchers who identified that it frequently tried to infect ASP (Active Server Pages) based websites. At the time the malware used command and control infrastructure hosted by the now-defunct **McColo Corp** ISP. After McColo was shut down, worldwide spam levels plummeted due to the disappearance of Asprox and other spam botnets, but they soon recovered.

By 2013, the primary components of Asprox had been replaced by a new malware family dubbed Kuluoz. While Asprox was an "all-in-one" malware, Kuluoz uses a modular design, which allows it to evade detection and gives attackers more flexibility. In May we identified a **new campaign** distributing Kuluoz that was generating over 30,000 new WildFire sessions per hour. Since that time Kuluoz has persisted to be highly prevalent across the entire world and the October data shows this pattern continues.

The constantly evolving Kuluoz family is currently known for the following:

- High distribution volume through geo location-associated spam e-mail templates
- Use of e-mail attachments and Web links that masquerade as document or media files
- **Modular design**, promoting extensibility
- Distinct roles for nodes in botnet including:
  - Spam generator for continued botnet propagation
  - Downloader of additional malware
  - Distributor of generalized commercial spam
- Platform-specific malware delivery based on user agent detection

E-mail themes for Kuluoz propagation spam have varied greatly and normally come in waves. These include legal notices (e.g., **court order**), **package delivery** messages (e.g., FedEx, UPS, DHL), voicemail service notifications (e.g., **WhatsApp**), current events (e.g., **2014 polar vortex**), and online deals (e.g., **free pizza from Pizza Hut**), to name just a few.

Much of Kuluoz's success is owed to its self-propagation feature and its selection of e-mail themes geared towards social engineering of targets. After Kuluoz infects a system, it immediately begins downloading additional components, which can take the following actions:

- Retrieve the latest spam templates and e-mail address list from the attacker and e-mail copies of itself to those addresses using the supplied template.
- Download and install additional malware that can earn money for the attacker (i.e. AdWare, RansomWare and Banking Trojans).
- Attempt to infect websites through known vulnerabilities.
- Steal e-mail, FTP and Web browser credentials from the infected system.

While the total number of Kuluoz sessions in October 2014 is very high, viewing this data on a daily basis (Figure 37) revealed a distinct pattern. Every weekend the total number of Kuluoz sessions drops close to zero, indicating that the systems responsible for sending much of the spam have stopped doing so, either on instructions from the attacker or by shutting down completely.

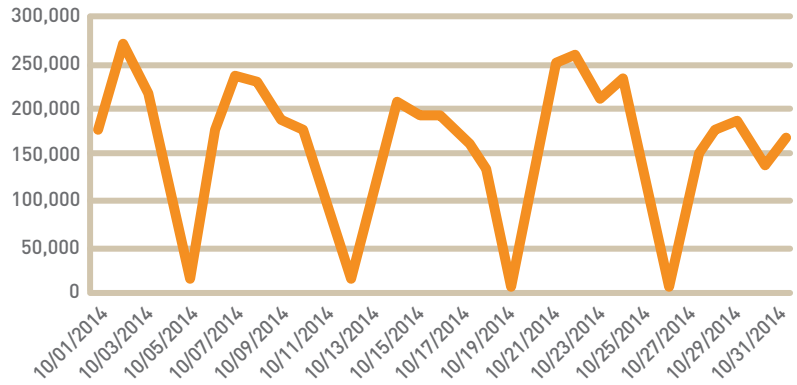


Figure 46: WildFire Kuluoz Detections (Total Sessions by Day)

A very similar pattern is apparent in the total number of unique Kuluoz samples detected throughout the month. The Kuluoz attackers stay ahead of antivirus detection by regularly regenerating the malware so that it frequently appears brand new, despite containing the same functionality.

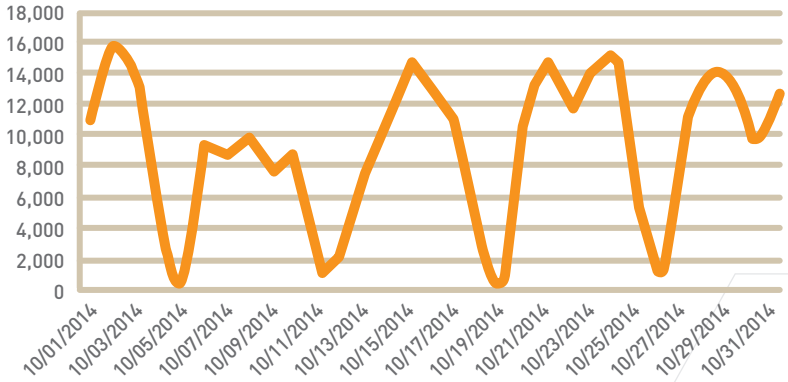


Figure 47: WildFire Kuluoz Detections (Unique Samples by Day)

Kuluoz is delivered as an Executable attachment in e-mail most commonly, but sometimes the executable is contained within a ZIP archive file. WildFire session data showed that in October the major e-mail protocols (SMTP, POP3, and IMAP) delivered 96% of the samples while web browsing and web-based applications accounted for the remaining 4%. FTP was observed in less the 1% of the sessions.

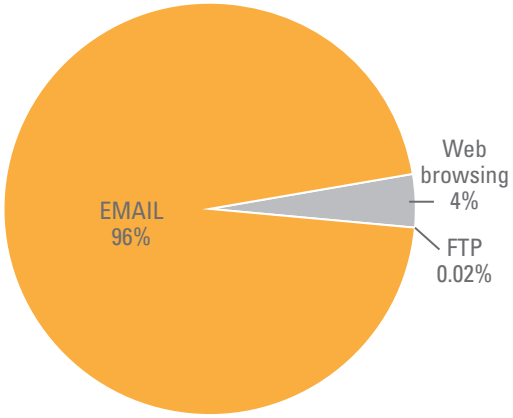


Figure 48: Proportion of sessions delivering Kuluoz for each App.

Every vertical examined in this report observed significant Kuluoz traffic over the month of October. The Higher Education, Healthcare, and High Tech sectors were the top three impacted industries.

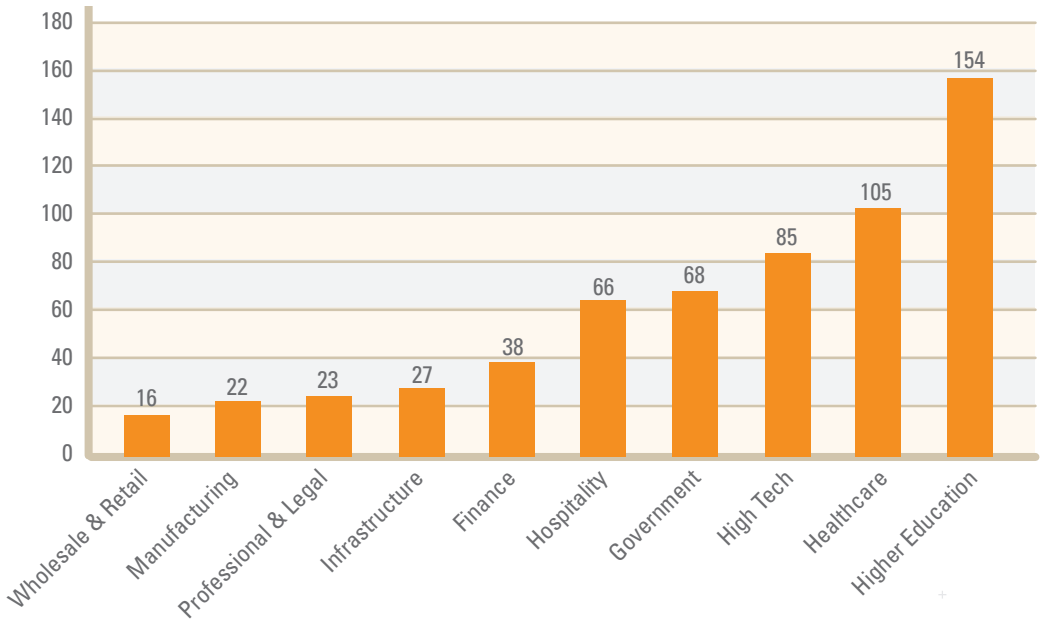


Figure 49: Average (mean) number of Kuluoz sessions per day for customers in each vertical.

As over 80% of the companies included in this report have experienced at least one attack from Kuluoz in the month of October, it's difficult to underestimate the overall impact of this botnet, which has proven itself extremely capable and boasts a long history of evading antivirus detection.

Defending Against Kuluoz

It is important that information security professionals and defenders are aware of the threats specific to their company and industry and stay up to date on the latest threat intelligence focused on their area. The following recommendations will ensure defenders are best poised for success:

- **User awareness:** Awareness and training for users will reduce the impact of any type of e-mail phishing. A number of Kuluoz variants require extra steps to be performed by a user (e.g., opening of a ZIP archive and then running a malicious binary). Encourage users to be wary of unexpected or unsolicited e-mails, especially those that employ any sort of pressure tactic and/or leverage the themes cited above.
- **Protocol monitoring and control:** Visibility into the protocols used by malware for delivery of Command and Control (HTTP, SMTP, IMAP, FTP) with structured and clearly defined response actions (most of which can and should be automated) to prevent or reduce associated impacts. Palo Alto Networks Next-generation Firewalls offer this level of granular application monitoring and control.
- **Automated analysis:** Automation of static and dynamic analysis for unknown samples addresses the natural gap between the development of a variant for a threat and its coverage through signature-based technology. Antivirus and other security control-related signatures fall short. Solutions such as Palo Alto Networks WildFire allow for enterprises to identify new and emerging threats that remain unknown to other security controls in the environment.
- **Intelligence fusion:** Leveraging actionable intelligence is a cornerstone of Computer Network Defense (CND) operations. Threats such as Kuluoz rely heavily on embedded initial Command and Control (C2) communications to fully realize the potential of its role(s) within the botnet. Up-to-date feeds on malicious domains, IPs, file signatures and hashes, as well as integration of intelligence gleaned from automated solutions in the environment, enable robust security solutions that empower network defenders.

4401 Great America Parkway
Santa Clara, CA 95054

Main: +1.408.753.4000
Sales: +1.866.320.4788
Support: +1.866.898.9087

www.paloaltonetworks.com