
# Cyber Threat Assessment:
# Threat Landscape Report Executive Summary

## A Look Behind the Firewall: An Industry Perspective on Key Usage and Threats from Inside America's Corporate Networks

The threat landscape is in a state of constant evolution. The rapid development of new malware, constant identification of critical flaws in software, rise of more organized and highly complex cybercriminal organizations and the high value of corporate data all contribute to the challenges faced by IT security leaders working hard to build and maintain the integrity of their critical corporate resources.

To stay ahead of the threats, cybersecurity professionals need to know what these hackers are after and understand the unique attack strategies that they employ as a result. Fortinet's CTAP: Threat Landscape Report takes a look at the overall threat environment and drills down into four key vertical industries.

This summary of the CTAP: Threat Landscape Report provides a brief overview and some of the key findings to reveal details about the current state of the threat landscape and provide industry-specific insights into the malicious tools and unique strategies that hackers tailor to each vertical industry.

## Data from Inside Live Business Networks

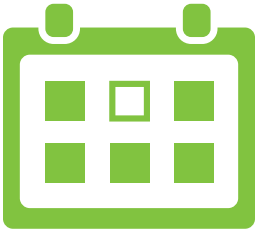
The data in this report was gathered from hundreds of US companies who participated in Fortinet's Cyber Threat Assessment Program (CTAP). CTAP is a global program that is free to all companies and was developed by Fortinet to allow enterprises to gain a deep understanding and incredible visibility into their network infrastructures.

To participate, each company installed FortiGate network security appliances behind their current security solutions for a period of three to seven days. The data represented in this report was collected from live production environments within a four-month timeframe. Fortinet's CTAP process provides each company with an individualized report that highlights critical gaps in their current security solutions and policies.

- The data in this report is anonymized and contains no identifiable information.
- The FortiGates were configured in "Transparent Mode" allowing them to capture and analyze the traffic passing through them without providing any security features or impacting network traffic.
- Participating companies ranged between small, medium, large and enterprise organizations in key industries including Education, Finance/Banking, Healthcare, and Technology.

## Industry-Wide Highlights: Overview of the Intersection of the Threat Landscape and Business Networks

- **32.14 Million Attempted Attack Events:** It's clear that enterprises of every size and vertical continue to face a constant and consistently hostile landscape.
- **71 Different Malware Variants Detected:** Utilizing increasingly sophisticated campaigns to expand their footprint, botnet activity is still dominant and a significant concern for security teams.
  - Botnets traditionally utilize two key vectors for infection: email attachments and compromised web content. However, we are starting to see indications of new strategies for infection that utilize instant messaging platforms to compromise user systems.
  - **5,230 instances of the Conficker botnet** topped the list of threats, followed by the **Nemucod Trojan** at **4,220 instances** and the Zeroaccess botnet taking the third spot with **3,210 instances**.
  - Botnets like these typically employ Trojans to compromise systems and then download additional payloads. As an example, Nemucod is notable for its use in campaigns to distribute new highly sophisticated and extremely lucrative ransomware, including Teslacrypt and Cryptolocker.



**32.14 Million**
Attempted Attack Events

**71 Malware**
Variants Detected

- **357,420 attempts to compromise applications** were detected within the top-10 list of application vulnerabilities alone.
  - Hackers cast a wide net to try and compromise corporate data, constantly scanning for known vulnerabilities in common operating systems, protocols, and applications in use today.

**357,420**
attempts to compromise applications

  - The top-10 list of application exploit attempts highlights how wide this net truly is, with the most frequently targeted operating systems including Linux, Unix, Mac OS X, and Windows—along with numerous open-source and proprietary operating systems and derivatives.

## Overall Network Usage Trends: What are Users Doing Inside the Network

- **25.65% of network traffic is used to browse social media or stream video and audio.** Fortunately, the rest of the traffic is put to productive uses like cloud-based applications, email, and system updates.
  - **YouTube makes up 42.29%** of streamed video/audio content on corporate networks. Video content served via HTTP combined with YouTube, Netflix, Hulu represent **80.89% of all video/audio streamed** within the workplace.
- **Facebook represents 47.27%** of all social media traffic, while most major social media platforms are accessed by users at work.
  - This can expose internal corporate systems and sensitive data to risks of infection from drive-by downloads, social engineering, and malvertising.
- **19.1% of traffic consists of advertising.** While difficult to avoid while browsing the Internet, advertising-based attack strategies have risen in popularity in recent years.

YouTube makes up
**42.29%**
of streamed video/audio content on corporate networks

Facebook represents
**47.27%**
of all social media traffic

## Industry-Specific Insights: Key Highlights and Callouts in the Top Industries

- **Banking and Finance saw the largest number of attack events** during the reporting period.
  - **44.6% of all malicious activity** was targeted at the Banking and Finance industry.
  - Banking and Finance organizations are disproportionately targeted due to the lucrative financial data obtained when these networks are successfully infiltrated.
  - **The Nemucod Trojan accounted for 46.8% of all malware activity** in the top 10 threats, with the list consisting entirely of various Trojans. Hackers are relying on high-velocity attacks, targeting financial institutions with sophisticated but relatively few malware variants.
  - The data demonstrates an emphasis on **land-and-expand attack strategies** designed to infiltrate and persist within the network. These Trojans then download additional banking-specific malicious payloads like Dyre or Zeus to extract as much information as possible.

**Banking & finance saw the largest number of attack events**

- **Education Organizations represented 27.4% of all attack events** in this report and came in second for overall malicious network activity.
  - **7 of the top 10 threat incidents were botnets** like Andromeda and Zeroaccess.
  - The data also reveals a couple threats that were unique to educational institutions:
    - **XcodeGhost,** the widely-publicized iOS malware, breaks into the top-10 vulnerabilities list in education. Apple aggressively remediated the issue and removed infected apps like WeChat from their store. This indicates that many users have not updated infected applications that they downloaded before September of 2015.
    - Hackers are scanning for **firmware flaws affecting ASUS wireless routers**, granting the hacker remote access. This can expose the network to malicious strategies like man-in-the-middle attacks. These consumer-oriented appliances are typically deployed in smaller organizations and wireless router firmware updates are often neglected due to the network downtime and manual effort required.

- **Healthcare ranked third** in overall malicious activity with **10.6% of attack events.**
  - Healthcare malware and botnet data closely mirror the land-and-expand strategy utilized to infiltrate and export data, with threat samples skewing heavily towards Trojans.
  - The healthcare industry is unique in the appearance of automated exploit kits, namely Angler and Nuclear, both of which target numerous vulnerabilities in Flash, Silverlight, and Internet Explorer to compromise a system via a drive-by-download or infected website.
    - Novel variants of both Angler and Nuclear exploit kits surfaced in late 2015 and have been tied to the delivery of far-reaching and **lucrative ransomware campaigns like TeslaCrypt and CryptoWall 4.0.**
    - This could indicate a shift in strategy from the more typical data exporting, to instead holding a healthcare organization's data inoperable until they pay the ransom. It seems that hackers feel they can receive a higher payout from the companies than they can when selling the information on the dark web.
- **The Technology Sector shared only 1.1% of overall attack activity.**
  - **Shellshock and Heartbleed top the list** of the most prevalent application vulnerabilities that affect technology industry networks.
  - **Trojans were again the primary tools employed by hackers.** The **Tepfer Trojan** was the second most prevalent malware variant in the list of top threats. This is an interesting case, as some variants of Tepfer target common instant messaging tools, along with FTP and email client applications.
  - The total number of threat events resulting from individual malware samples was distributed much more evenly than many of the other industries in the report. This indicates that hackers are casting a wide net and relying on automated and/or pay-per-install strategies to try and compromise technology businesses.

FORTINET

GLOBAL HEADQUARTERS
Fortinet Inc.
899 Kifer Road
Sunnyvale, CA 94086
United States
Tel: +1.408.235.7700
www.fortinet.com/sales

EMEA SALES OFFICE
905 rue Albert Einstein
Valbonne
06560, Alpes-Maritimes,
France
Tel +33 4 8987 0500

APAC SALES OFFICE
300 Beach Road 20-01
The Concourse
Singapore 199555
Tel: +65.6513.3730

LATIN AMERICA SALES OFFICE
Paseo de la Reforma 412 piso 16
Col. Juarez
C.P. 06600
México D.F.
Tel: 011-52-(55) 5524-8428



Feb 17, 2016