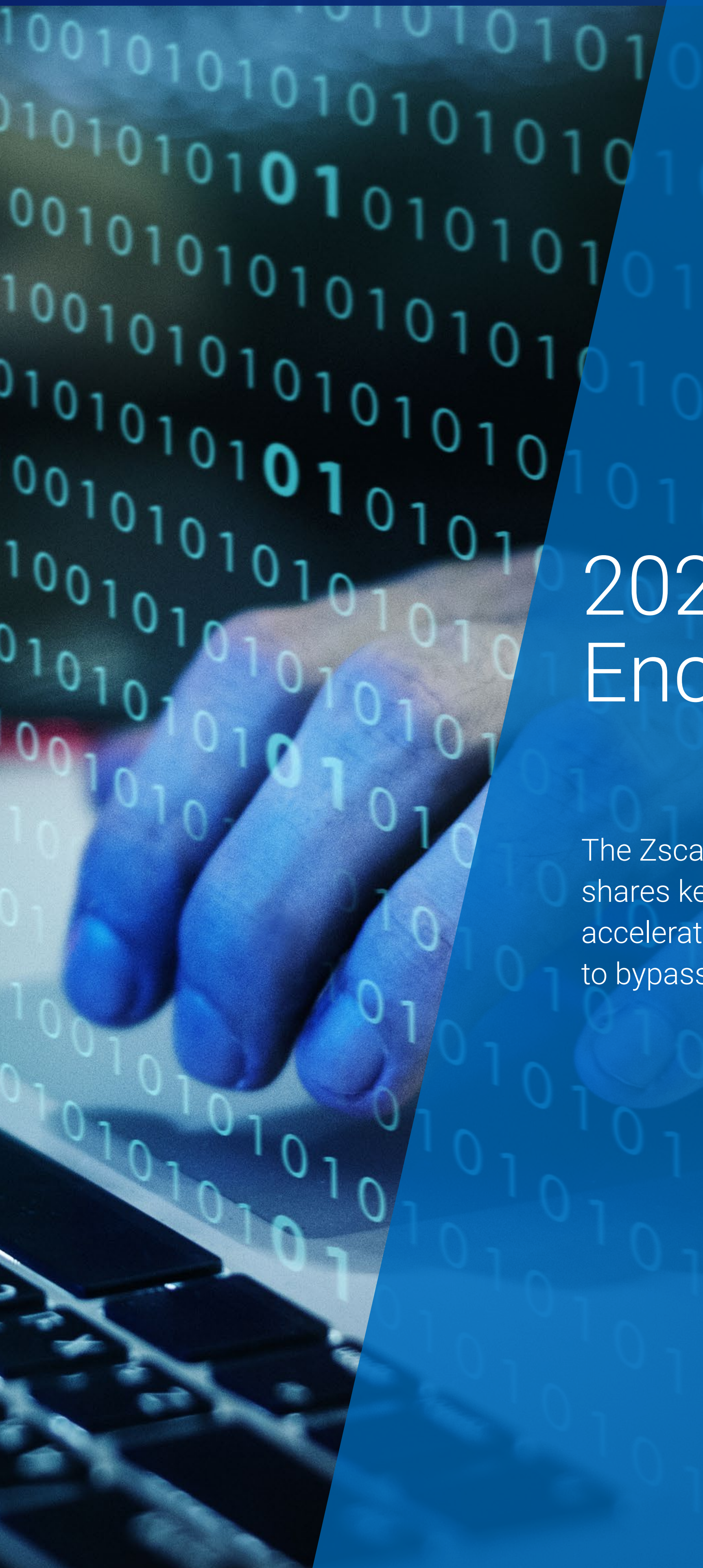


2020 State of Encrypted Attacks

The Zscaler™ ThreatLabZ research team shares key insights on how attackers are accelerating their use of SSL/TLS encryption to bypass traditional defenses

JANUARY–SEPTEMBER 2020

Contents

About ThreatLabZ

ThreatLabZ is the global security research team at Zscaler. In addition to its work protecting Zscaler customers from emerging threats, the team analyzes the enterprise traffic that crosses the Zscaler cloud. With the team's expertise in cybersecurity, data science, and AI/machine learning—along with the volume of data analyzed from more than 120 daily billion transactions in Zscaler's Zero Trust Exchange™ cloud platform—ThreatLabZ is uniquely positioned to provide insight into enterprise traffic and security trends.

When ThreatLabZ discovers a new attack campaign or malware with uncommon techniques or capabilities, researchers detonate these files and analyze their code to see exactly how they are programmed to evade detection, drop payloads, steal information, control devices, spy on the user, propagate, and spread. We make the results of our analyses freely available to the security community on the **Zscaler research blog**.

Specific to SSL trends, ThreatLabZ researchers recently uncovered, analyzed, and reported on threats leveraging encrypted channels, which you can read about in the following posts:

> Fake VPN Sites Deliver Infostealers

> Abuse of StackBlitz Tool to Host Phishing Pages

> JavaScript Skimmers

> Higaisa Advanced Persistent Threat

To see the Zscaler cloud in action, view the **Cloud Activity Dashboard**, which displays the number of transactions being processed and threats being blocked every second.

INTRODUCTION:

SSL traffic is hiding malware. A lot of it.

Much to the irritation of security experts, there's a belief about SSL encryption that is as persistent as it is misguided: "I thought, as long as a website was using SSL encryption, it would be safe."

SSL encryption was designed to protect traffic from prying eyes, but adversaries have also leveraged it to hide attacks, turning the use of encryption into a potential threat without proper inspection.

Cybercriminals know what security experts know: that SSL/TLS encryption is the industry-standard way to protect data in transit. Those same cybercriminals use industry-standard encryption methods themselves, devising clever ways to hide malware inside encrypted traffic to carry out attacks that bypass detection. In fact, between January and September, the Zscaler cloud blocked an astounding 6.6 billion security threats hidden inside encrypted traffic, which amounts to an average of 733 million blocked per month. This monthly average is an increase of nearly 260 percent over 2019, when the Zscaler cloud was blocking an average of 283 million threats per month in encrypted traffic.

Inspecting encrypted traffic must be a key component of every organization's security defenses. The problem is that traditional on-premises security tools like next-generation firewalls struggle to provide the performance and capacity needed to decrypt, inspect, and re-encrypt traffic in an effective manner. Attempting to inspect all SSL traffic would bring performance (and productivity) to a grinding halt, so many organizations allow at least some of their encrypted traffic to pass uninspected, such as traffic from cloud service providers and others deemed to be "trusted." This is a critical shortcoming. Failing to inspect all encrypted traffic leaves organizations vulnerable to hidden phishing attacks, malware, and more, all of which could be disastrous.

Between January and September, the **Zscaler cloud identified and stopped 6.6 billion threats** hidden inside encrypted traffic.

The ThreatLabZ team analyzed encrypted traffic across the Zscaler cloud for the first nine months of 2020, assessing its use within specific industries. The goal of the analysis is to understand not only the volume of traffic that uses encryption, but also the threats hidden within that traffic. Some of the highlights include:

- **The majority of internet traffic is encrypted:** 80% of all traffic uses SSL/TLS encryption by default.
- **Explosive growth in volume:** 260% increase in SSL-based threats in the last nine months, accelerated by the spike in cloud-based collaboration apps during COVID-19.
- **Healthcare under attack:** Healthcare was the most targeted industry, with 1.6 billion encrypted threats identified and stopped, followed by finance and manufacturing.
- **Increasing abuse of cloud-based file-sharing services:** Over 30% of all SSL-based attacks hide in collaboration services such as Google Drive, OneDrive, AWS, or Dropbox.
- **Hidden ransomware on the rise:** More than 5x increase in ransomware delivered in encrypted web traffic.

Cybercriminals use SSL/TLS too: Why inspecting encrypted traffic is important

Encrypting internet traffic via SSL (Secure Sockets Layer), and its more modern replacement TLS (Transport Layer Security), is the global standard for protecting data in transit, and the vast majority of internet traffic today is encrypted.[1] The problem is that criminals are using encryption, too, to hide malware and other exploits. This means that traffic moving through encrypted channels can no longer be trusted simply by virtue of a digital certificate.

Cybercriminals have created sophisticated attack chains that start with an innocent-looking phishing email containing an exploit or hidden malware. If an unsuspecting user clicks, then the attack moves into the malware installation phase, and ultimately to the exfiltration of valuable corporate data.

What makes the attacks so nefarious is that the exploit or hidden malware is encrypted, too, which changes its file structure completely. Cybersecurity systems rely on a file's structure (or "fingerprint") to identify incoming threats; if it's structured a certain way, the system knows to block it. But each time a file is encrypted, it gets a brand-new fingerprint that isn't recognized as a threat.

SSL inspection is the only effective way to block the malicious files delivered [using these services], because security engines cannot block what they can't see.

[1] https://transparencyreport.google.com/https/overview?hl=en

SSL traffic trends

Enterprises have largely accepted the fact that encryption is a requirement for protecting data in transit from interception and exploitation. In our analysis, we found that the education sector encrypted the highest percentage of its traffic, followed by manufacturing, finance, and healthcare. But all industries, including retail/wholesale, services, technology-communication, and government are bunched pretty closely together. During the analysis period, between January and September 2020, we saw the use of encryption across all industries averaging about 75 percent and peaking at more than 80 percent.

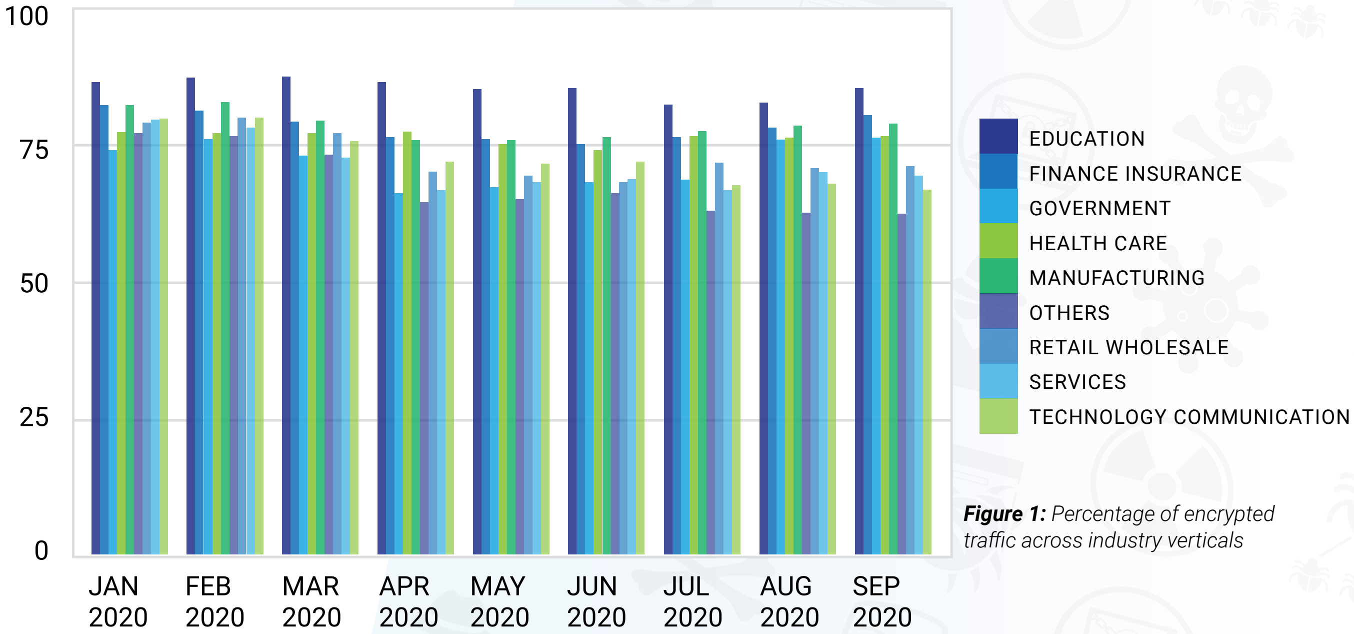


Figure 1: *Percentage of encrypted traffic across industry verticals*

High rates of encrypted traffic were observed across every industry vertical, meaning all organizations must consider how to inspect SSL/TLS for threats.

According to our research, threat actors target healthcare with encrypted malware attacks more than any other sector. Between January and September 2020, the healthcare sector accounted for 25.5 percent of all advanced threats blocked over encrypted channels in the Zscaler cloud, followed by finance/insurance at 18.3 percent, manufacturing at 17.4 percent, and government at 14.3 percent.

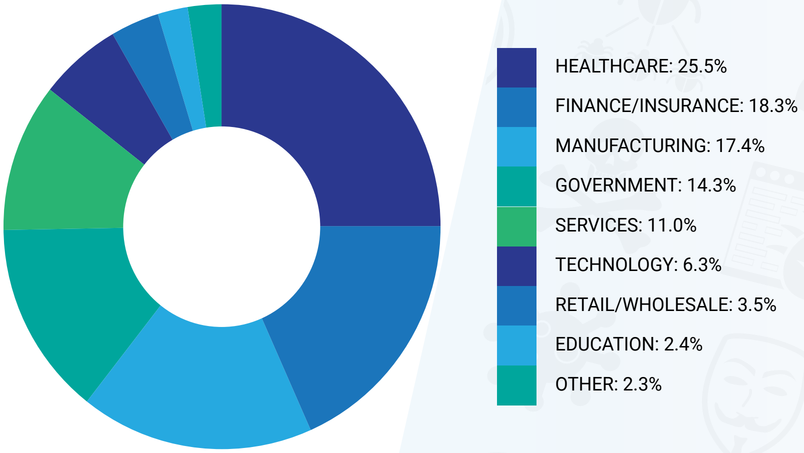


Figure 2: *Advanced threats blocked over encrypted channels by industry*

Healthcare organizations were targeted with the most threats delivered over encrypted channels, despite the global pandemic making their services more critical than ever. Attackers have also used the pandemic to launch new campaigns, with fake sites offering news, products, and cures. In the first three months of 2020, ThreatLabZ reported a **30,000 percent** spike in COVID-related threats.

Industry focus—healthcare

The healthcare sector was the target of more than 1.69 billion attempted attacks over encrypted channels during our analysis—more than any other sector. The vast majority of the attacks on this sector came via malicious URLs (84.2 percent). Malicious URLs can be delivered to users via email, text message, pop-ups, or on-page advertisements, leading to downloaded malware, spyware, ransomware, compromised accounts, and more.

The healthcare industry is often the target of cyberattacks, because of the presence of legacy systems (due to prolonged FDA approval) in the environment. These legacy systems lack security controls and are often vulnerable to known issues. Without unified controls and centralized visibility and policy enforcement, such organizations wind up with gaps in their security controls that cybercriminals attempt to take advantage of.

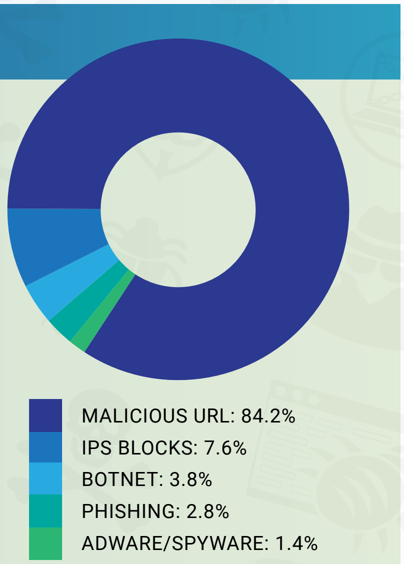


Figure 3: *Threats over encrypted channels targeting the healthcare sector*

Attacks are becoming more advanced

Users are often warned by IT professionals to carefully check the URL of a suspected fake site for errors, misspellings, or other indicators that they may not be legitimate. But these days, cybercriminals are taking advantage of techniques such as domain squatting and IDN homograph attacks to make their sites look virtually indistinguishable from the real ones.

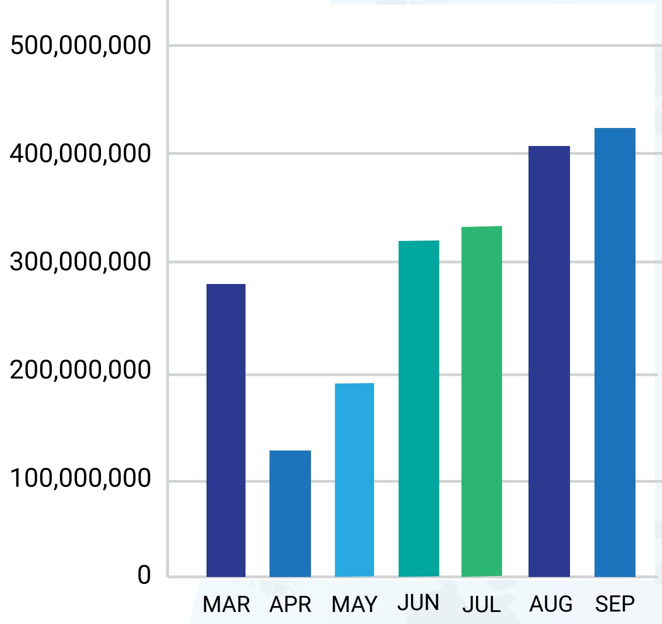
Domain squatting is registering a top-level domain that is similar to a known brand (such as gmali.com) for the purpose of phishing, stealing credentials, or serving malware.

A homograph attack, like domain squatting, is used to trick people into clicking links by using characters, such as the numeral “1” instead of an “l” in the Apple URL (https://www.app1e.com).

Abuse of cloud storage services

Cloud storage services have emerged as a popular means of attack. These services are great for securely sharing files via SSL-based transmission on the web. But since cybercriminals know that most organizations are unable to inspect SSL traffic at scale, and that cloud services are generally “trusted,” they launch attacks that appear to originate from these services.

From March through September 2020, the Zscaler cloud blocked **two billion threats** in encrypted traffic, the majority of which involved malicious content hosted on Google, AWS, Dropbox, and OneDrive. These threats nearly doubled between March and September and accounted for almost 30 percent of all SSL/TLS encrypted threats in those months.



From March through September, the Zscaler cloud blocked **two billion threats** in SSL traffic originating from cloud storage service providers.

Figure 4: *Advanced threats blocked over TLS/SSL from top cloud storage services*

Figure 5 shows how cloud services are exploited to host and serve malware. Cybercriminals upload the malware payload (often a stage 1 downloader file) on one or more services and distribute the URLs as part of an email spam campaign. The use of leading services such as Google, Microsoft, Amazon, and Dropbox improve the chances of end users clicking the link.

Cybercriminals also take advantage of the wildcard SSL certificates belonging to these service providers. If cloud-provider traffic is assumed safe and goes uninspected, it helps bad actors serve malware payloads over encrypted channels and evade URL filtering-based security solutions such as anti-spam, email protection, firewalls, and more. **A phishing email with a link to a malicious file hosted in a trusted cloud-based service can evade traditional email security solutions.**

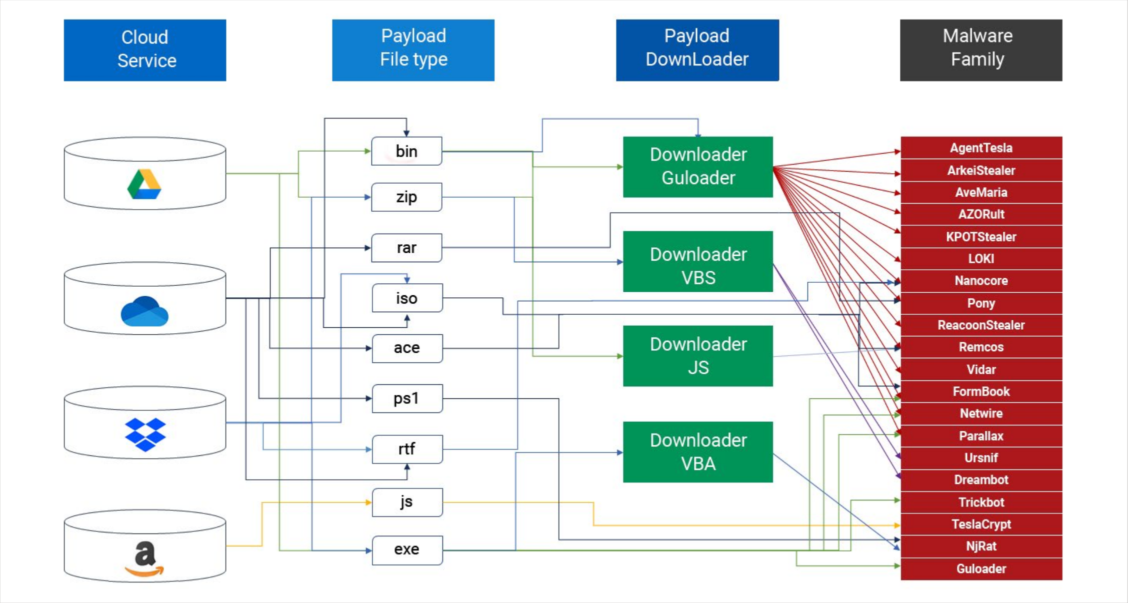
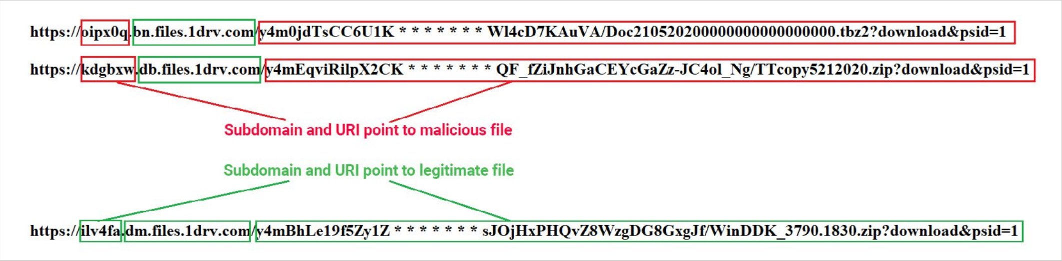


Figure 5: *Malware payloads delivered via cloud services*

The example below shows URLs from the OneDrive cloud storage service. In this example, the first two URLs are malicious and result in the downloading of malware belonging to the "Trojan EdLoader" and "Backdoor LokiBot" families. However, the third URL is legitimate and downloads the user's actual file. The subdomain and Uniform Resource Identifier (URI) appear as random string patterns that make it impossible to distinguish legitimate URLs from malicious ones. SSL inspection is the only effective way to block the malicious files delivered using these services, because security engines cannot block what they can't see.



https://oipx0q.bn.files.1drv.com/y4m0jdTsCC6U1K * * * * * * * Wl4cD7KAuVA/Doc210520200000000000000.tbz2?download&psid=1

https://kdgbxw.db.files.1drv.com/y4mEqviRilpX2CK * * * * * * * QF_fZiJnhGaCEYcGaZz-JC4ol_Ng/TTcopy5212020.zip?download&psid=1

Subdomain and URI point to malicious file

Subdomain and URI point to legitimate file

https://ilv4fa.dm.files.1drv.com/y4mBhLe19f5Zy1Z * * * * * * * sJOjHxPHQvZ8WzgDG8GxgJf/WinDDK_3790.1830.zip?download&psid=1

Figure 6: *Random strings in subdomains make it impossible to distinguish malicious URLs from legitimate ones*

Mobile attacks

Smartphones have also become popular targets. In the same way that cybercriminals spoof web pages, they create fake apps that look legitimate. For example, an Android banking trojan called Cerberus uses an application name and icon to mimic the legitimate Google Play application. After an unsuspecting user clicks on the fake app, it sends out a notification to gain "accessibility service" permission. (Accessibility service assists users with disabilities in using Android devices and apps.)

This exploit assumes that many users will "accept" a notification without carefully reading it. In this case, clicking "Allow" lets the app view the content of other apps displayed on the screen and perform a variety / of actions without the user's knowledge.

The malware grabs the credentials of banking apps, Gmail, or the Google Authenticator two-factor authentication app, and then exfiltrates them. It can also take other sinister actions, such as stealth audio recording and stealing text messages. It gets worse. After accessibility service permission is granted to the malware, it can prevent the user from disabling the permission and can make it difficult to uninstall the app.

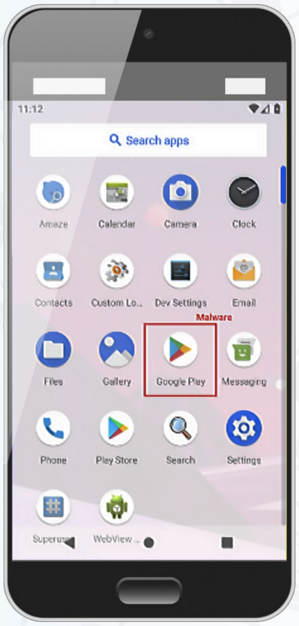
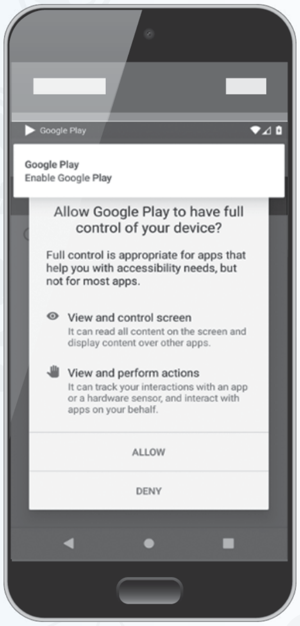


Figure 7: *Fake Google Play app*



Google Play
Enable Google Play

Allow Google Play to have full control of your device?

Full control is appropriate for apps that help you with accessibility needs, but not for most apps.

View and control screen
It can read all content on the screen and display content over other apps.

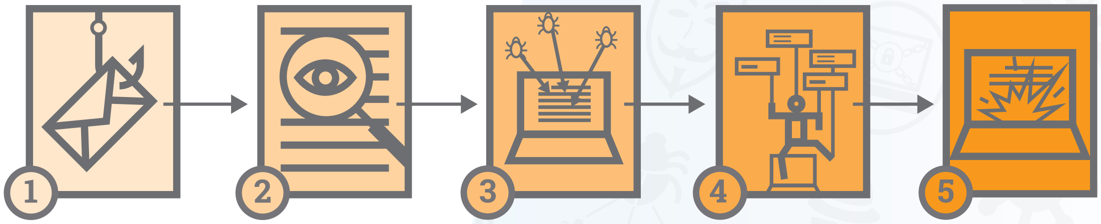
View and perform actions
It can track your interactions with an app or a hardware sensor, and interact with apps on your behalf.

ALLOW

DENY

Figure 8: *Notification on fake Google Play app*

Anatomy of an attack



1. **Delivery** may include a phishing email with an exploit or malware hidden inside. The malware is delivered when a user downloads it or clicks a link in the email.
2. **Exploitation** is what happens as the program looks for vulnerabilities in the system it can exploit and execute the code.
3. **Installation** occurs when the malware is loaded onto the victim's machine.
4. **Command-and-control (C&C) callback** is when malware attempts to communicate with C&C servers, often to get instructions or to send stolen data.
5. **Detonation** is the step in which the malware may install additional malware, exfiltrate data, or perform other actions programmed by the C&C server.

Analyzing the attack chain

Phishing

Since phishing is typically the first stage of a multistage cyberattack involving credential theft, we analyzed the more than **193 million phishing attempts** delivered over encrypted channels but identified and blocked by the Zscaler cloud between January and September 2020. We broke down the attempts by industry verticals. With individual facilities often using different IT infrastructures and systems (making them potentially more vulnerable), the manufacturing sector was the highest-profile target, receiving 38.6 percent of the phishing attempts, followed by services at 13.8 percent.

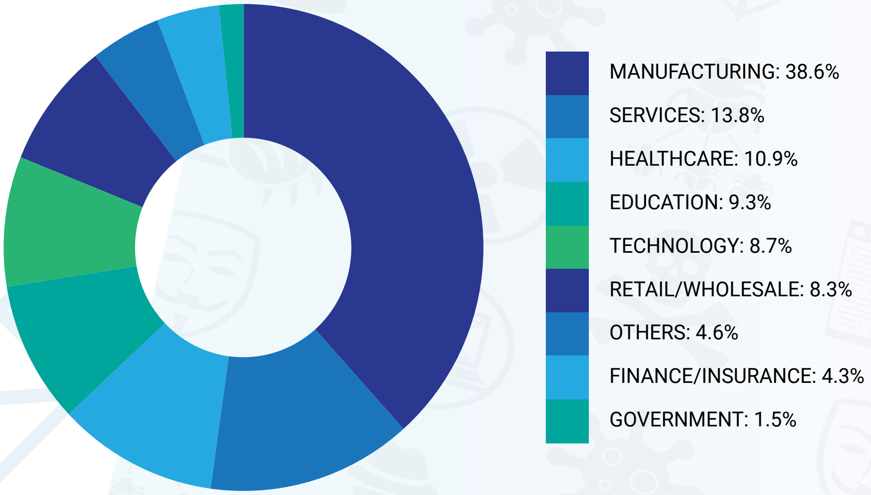


***Figure 9:** Phishing threats blocked over encrypted channels, by industry*

Corporate services and brands being phished

A phishing attempt frequently includes a spoofed website that mimics a targeted brand. In other words, an email arrives and instructs the user to click on a link that takes the user to a fake website. There, the user is instructed to enter a user name/password or other critical information that can be used by cybercriminals to carry out attacks.

Our research found that the most-phished brand was Microsoft. Attacks feature various Microsoft-themed web properties (Office 365, SharePoint, OneDrive, etc.), with which cybercriminals try to steal corporate service credentials. The second-most popular phishing attacks involved "Tech Support" scams, which typically use a malicious web redirect from compromised websites that claim the user's machine has been hacked and that "Microsoft support" will fix it (once credit card information has been submitted by the user).

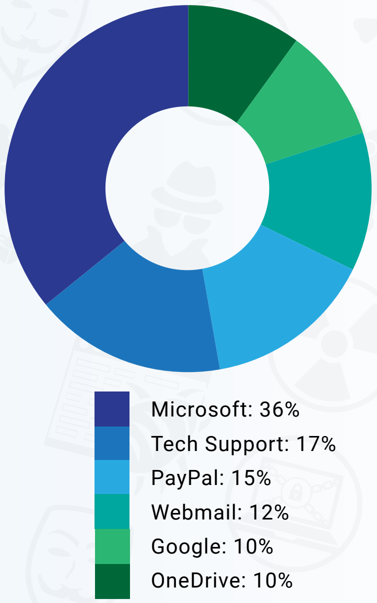
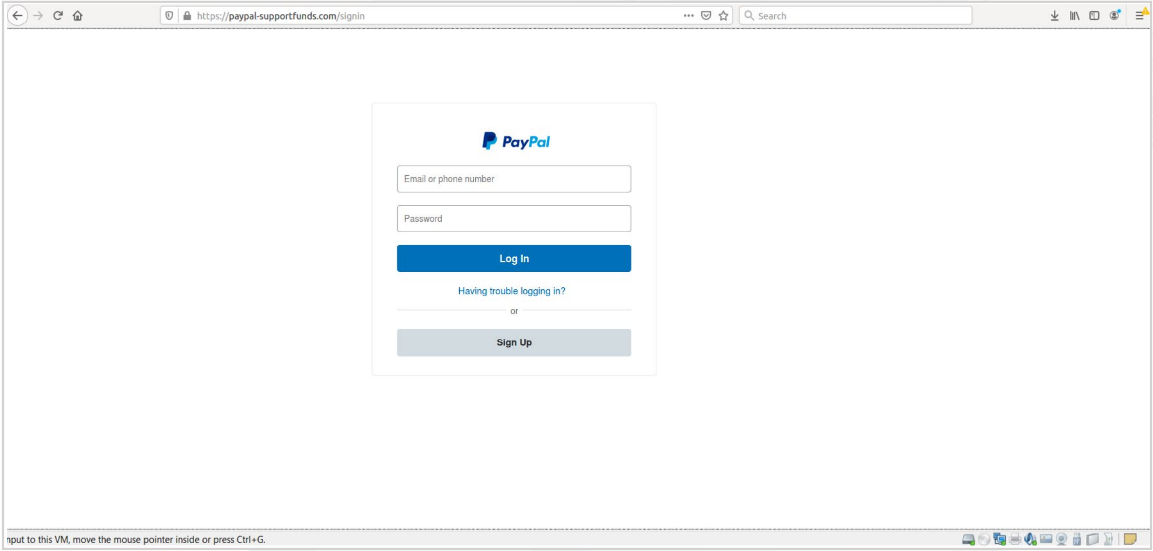


Figure 10: *Corporate brands and services most frequently phished*

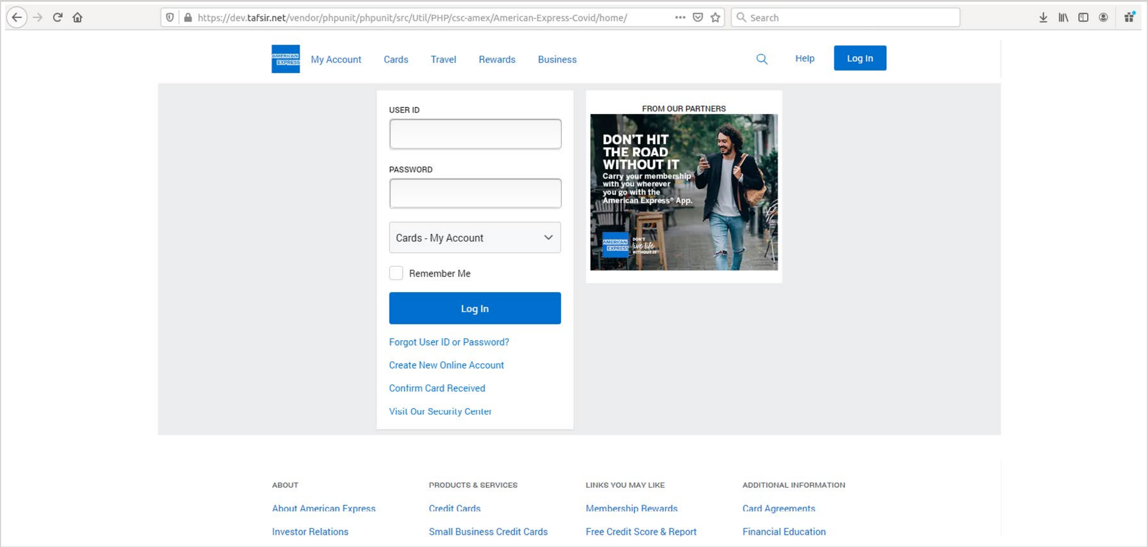
PayPal and Google were also among the top brands spoofed by these phishing attacks. The spoofed sites look eerily similar to the real sites, making spotting the fakes difficult.



https://paypal-supportfunds.com/signin

nput to this VM, move the mouse pointer inside or press Ctrl+G.

Figure 11: *PayPal phishing site over HTTPS*



https://dev.tafsir.net/vendor/phpunit/phpunit/src/Util/PHP/csc-amex/American-Express-Covid/home/

Search
AMERICAN EXPRESS
My Account
Cards
Travel
Rewards
Business
Help
Log In

USER ID

PASSWORD

Cards - My Account

□ Remember Me

Log In

Forgot User ID or Password?

Create New Online Account

Confirm Card Received

Visit Our Security Center

FROM OUR PARTNERS
DON'T HIT THE ROAD WITHOUT IT
Carry your membership with you wherever you go with the American Express® App.

ABOUT	PRODUCTS & SERVICES	LINKS YOU MAY LIKE	ADDITIONAL INFORMATION
About American Express	Credit Cards	Membership Rewards	Card Agreements
Investor Relations	Small Business Credit Cards	Free Credit Score & Report	Financial Education

Figure 12: *American Express phishing site over HTTPS*

Netflix phishing over HTTPS

The use of streaming entertainment services such as Netflix has increased during the pandemic—and cyberattackers have noticed. Bad actors target streaming services to phish for user credentials. And, as seen in Figure 13, it is difficult to distinguish these fake pages from real ones.

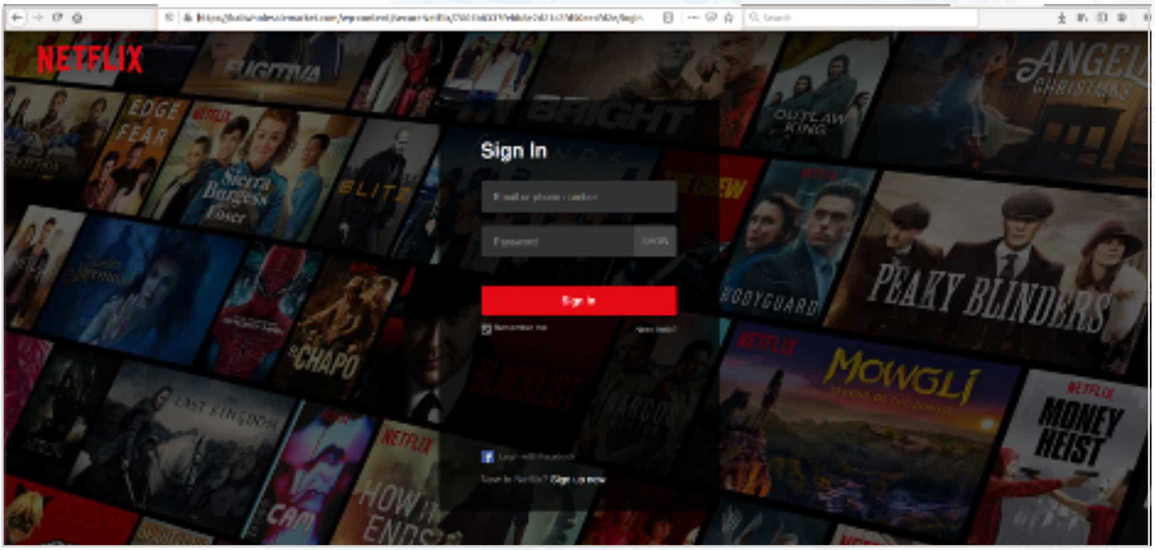
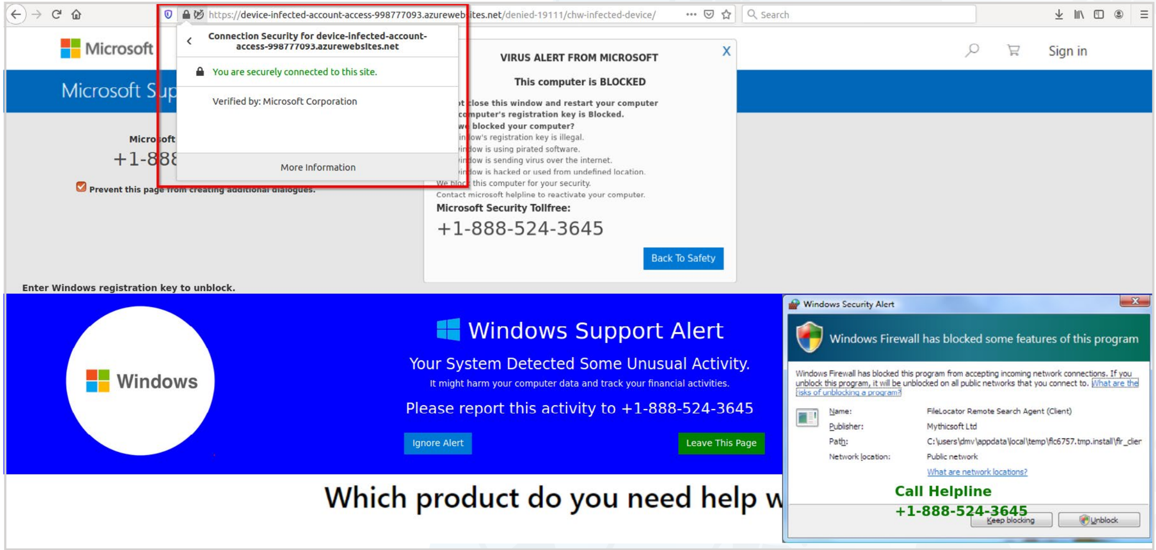


Figure 13: *Netflix phishing image*

Tech support scam over HTTPS targeting Microsoft users

Figure 14 shows a Microsoft tech support scam page. Clicking on the URL shows the HTTPS certificate as verified by Microsoft. The certificate being used shows that the attackers are leveraging Azure (another well-known brand) in an attempt to add the appearance that this is a legitimate page sent by Microsoft.



https://device-infected-account-access-998777093.azurewebsites.net/denied-19111/chw-infected-device/

Connection Security for device-infected-account-access-998777093.azurewebsites.net

You are securely connected to this site.

Verified by: Microsoft Corporation

More Information

Microsoft

Microsoft Sup

Micro soft

+1-888

☑ Prevent this page from creating additional dialogues.

VIRUS ALERT FROM MICROSOFT

This computer is BLOCKED

...t close this window and restart your computer
...computer's registration key is Blocked.
...we blocked your computer?
...indow's registration key is illegal.
...indow is using pirated software.
...indow is sending virus over the internet.
...indow is hacked or used from undefined location.
We block this computer for your security.
Contact microsoft helpline to reactivate your computer.

Microsoft Security Tollfree:

+1-888-524-3645

Back To Safety

Enter Windows registration key to unblock.

Windows

Windows Support Alert

Your System Detected Some Unusual Activity.

It might harm your computer data and track your financial activities.

Please report this activity to +1-888-524-3645

Ignore Alert

Leave This Page

Which product do you need help w

Windows Security Alert

Windows Firewall has blocked some features of this program

Windows Firewall has blocked this program from accepting incoming network connections. If you unblock this program, it will be unblocked on all public networks that you connect to. What are the risks of unblocking a program?

Name: FileLocator Remote Search Agent (Client)
Publisher: Mythicsoft Ltd
Path: C:\users\dmv\appdata\local\temp\flc6757.tmp.install\flr_clier
Network location: Public network

What are network locations?

Call Helpline
+1-888-524-3645

Keep blocking

Unblock

Figure 14: *Tech support scam over HTTPS targeting Microsoft users*

Browser exploits

Browser exploits allow attackers to take advantage of a vulnerability in an operating system and change a user's browser settings without that user's knowledge. The Zscaler cloud blocked more than 658,000 browser exploitation threats targeting manufacturing (26.5 percent) and finance/insurance (19.9 percent), the top targets.

The manufacturing industry is often the target of cyberattacks because (traditionally, at least) this industry was highly fragmented, with individual facilities each using different IT infrastructures and multiple disjointed systems. As in other industries, without unified controls and centralized visibility and policy enforcement, security is incomplete and cybercriminals continue to exploit these holes.

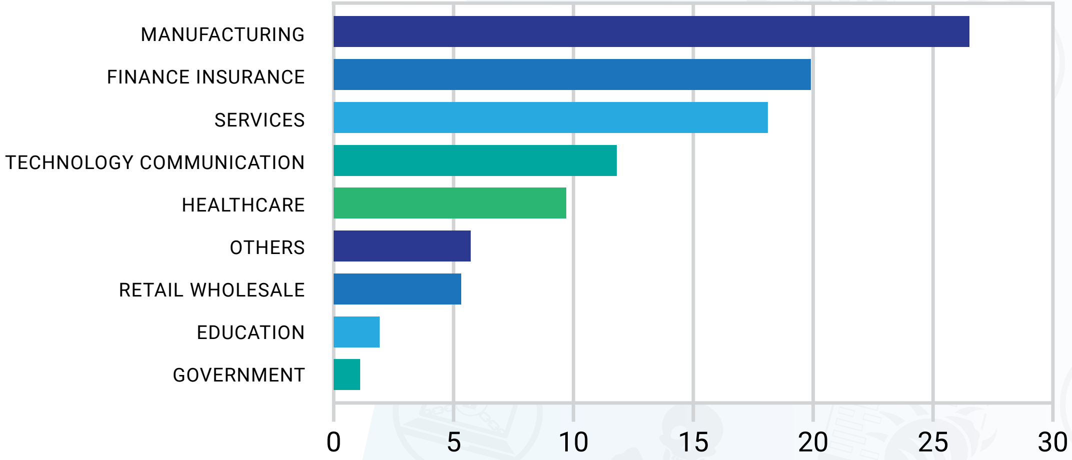


Figure 15: *Browser exploits blocked over encrypted channels by industry*

Ransomware

Zscaler ThreatLabZ has seen ransomware attacks delivered over SSL/TLS channels increase 500 percent since March 2020. With the majority of employees working remotely and accessing internal applications, there has been an increase in ransomware activity targeting industry verticals that are more susceptible and likely to pay ransoms.

Technology/Communication (40.5) and healthcare (26.5) were among the most targeted industry verticals by ransomware attacks over encrypted channels.

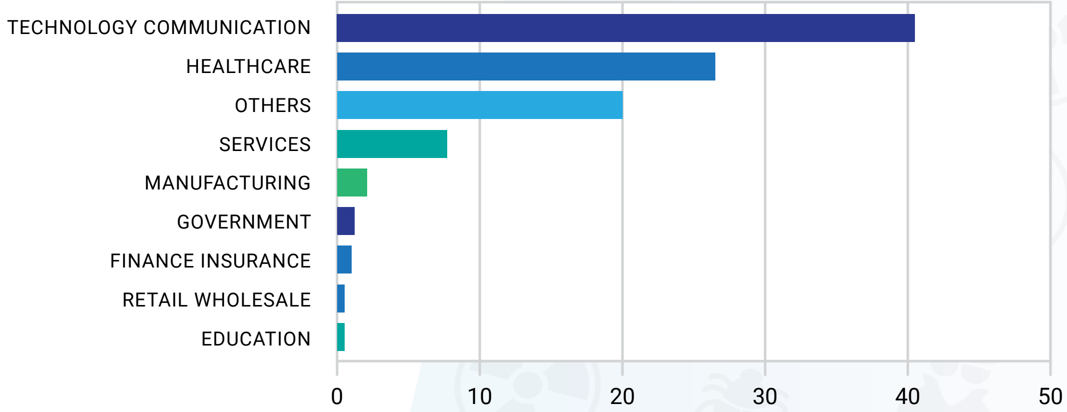


Figure 16: *Ransomware blocked over encrypted channels by industry*

The top ransomware families seen in these attacks include FileCrypt/FileCoder variants, followed by Sodinokibi, Maze, and Ryuk family variants. A notable change in many of these ransomware family variants during the past year has been the addition of a data exfiltration feature. This new feature allows ransomware gangs to exfiltrate sensitive data from victims before encrypting the data. This exfiltrated data is like an insurance policy for attackers: even if the victim organization has good backups, they'll pay the ransom to avoid having their data exposed.

Malware

Malware provides a means of persistence, which enables a cybercriminal to have continued access to a victim's machine. Malware is often installed upon successfully exploiting vulnerabilities or via social engineering attacks. It is by far the attack type identified most often by Zscaler researchers, with more than **2.6 billion malware threats** blocked during our analysis.

Industries that handle personally identifiable information (PII) are frequent targets of malware, and in our analysis, healthcare and finance/insurance had the most malware attacks blocked over encrypted channels at 27.4 and 19.6 percent, respectively.

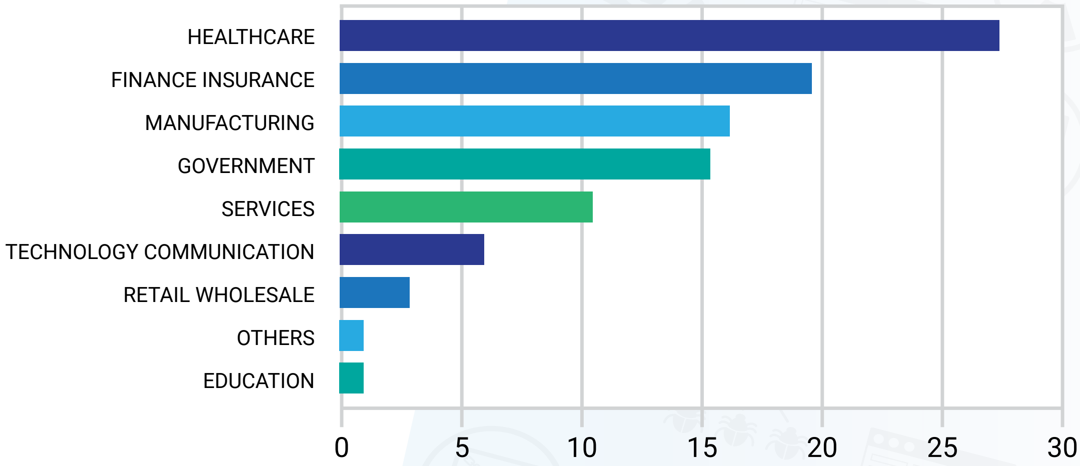


Figure 17: *Malware blocked over encrypted channels by industry*

Malware command-and-control (C&C) activity over encrypted channels

C&C communication is another key part of the attack chain. If the malware has avoided detection and is successfully installed on an end user's device, it calls back to the C&C server to begin exfiltrating data and launching further attacks. Malware payloads are often programmed to remain dormant and await commands from the server before initiating any malicious activities. Emotet and TrickBot were the two most prevalent malware families seen in our analysis.

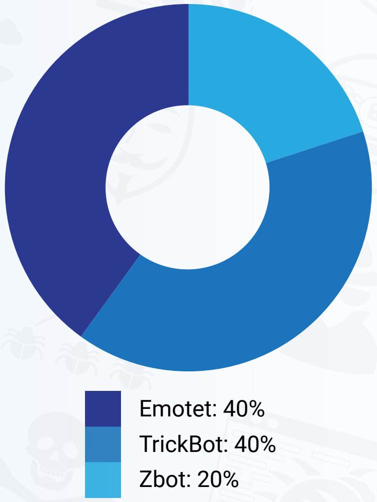


Figure 18: *Most commonly blocked C&C activity over encrypted channels*

In addition to Emotet and TrickBot, we saw activity from Ursnif and Unruy. Emotet was the most widely used across all industries, while TrickBot was the second most commonly used type of malware in finance/insurance and government. Ursnif was popular in attacks on healthcare and manufacturing, while Unruy was the second most used type of malware in attacks on educational institutions.

Get to know your malware

Emotet: Emotet started as a banking trojan in 2014. However, it has morphed into a very prominent threat used mostly for spamming and downloading malware on target systems. The U.S. Cyber Infrastructure Security Agency (CISA) called Emotet among the **most costly and destructive** malware strains affecting both the public and private sectors. Emotet has proven itself to be resilient and modular, with regular enhancements that make it difficult for organizations to detect.

TrickBot: TrickBot is a successor to the banking trojan Dyre and has become one of the most prevalent and dangerous malware strains in today's threat landscape. Often seen working with other types of malware, TrickBot is sometimes used as an initial infection vector to find its way into the target host or to download other malware families to get the most out of an infection.

Ursnif: The Ursnif trojan is one of the most active and prevalent variants of the Gozi malware family, also known as Dreambot. The trojan is often spread by exploit kits, email attachments, and malicious links.

Unruy: Unruy is a trojan that displays out-of-context advertisements and performs ad-clicking in order to gather revenue for its controllers. It communicates with remote hosts and may also download and execute arbitrary files to carry out its activities.

What’s needed to prevent encrypted threats

It’s increasingly important to recognize that SSL traffic is not necessarily secure traffic. Just as the use of encryption has increased, so has its use among adversaries to hide their attacks. The need to inspect encrypted traffic is greater than ever. Many organizations follow security best practices and encrypt their internet traffic. However, legacy tools like next-generation firewalls often lack the performance and capacity to inspect SSL traffic at scale. No one can afford to bring operations and workflows to a grinding halt, so many IT teams allow most encrypted traffic to pass uninspected.

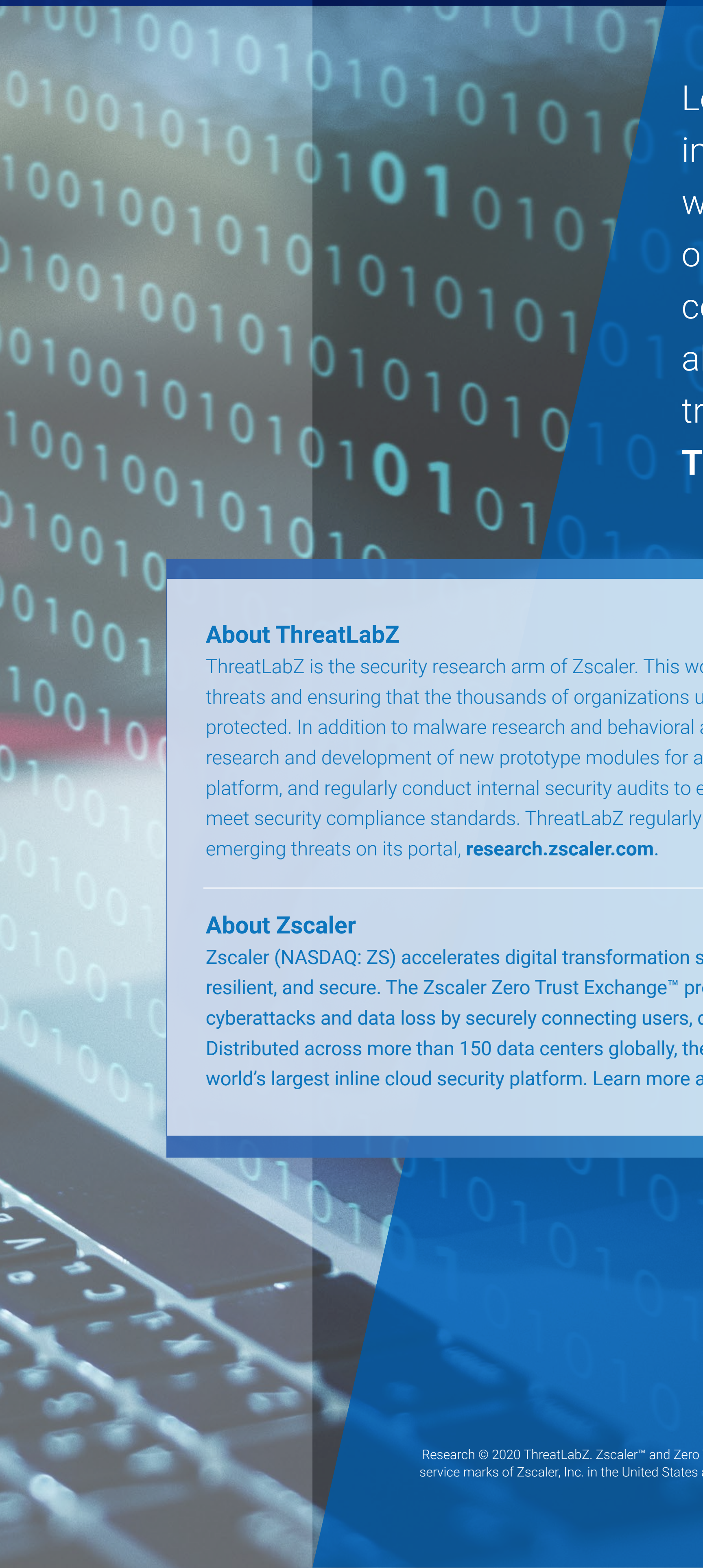
In addition, there are strict regulations regarding how organizations must treat data that contains personal information about customers, patients, and so on. Creating separate policies for how specific types of data are to be inspected and replicating it at different locations is an arduous task, so organizations often skip the process altogether.

So how can you protect your organization from the dangers hidden within encrypted traffic—without the performance hit? With the majority of enterprise traffic now encrypted, how can you be sure to decrypt and inspect all of it, while maintaining compliance, for all users on and off the network?

- **Decrypt, detect, and prevent threats in all SSL traffic** with a cloud-native proxy-based architecture that can inspect all traffic for every user.
- **Quarantine unknown attacks and stop patient-zero malware** with AI-driven quarantine that holds suspicious content for analysis, unlike firewall-based passthrough approaches.
- **Provide consistent security for all users and all locations** to ensure everyone has the same great security all the time, whether they are at home, at headquarters, or on the go.
- **Instantly reduce your attack surface** by starting from a position of zero trust, where lateral movement can’t exist. Apps are invisible to attackers, and authorized users directly access needed resources, not the entire network.

The solution requires the scalability and performance that can only be delivered by a cloud-native, proxy-based architecture such as the Zscaler Zero Trust Exchange. A cloud-based security platform meets the demands of decryption and inspection by elastically scaling computing resources, and provides consistent policy enforcement across multiple locations. Zscaler performs SSL inspection at scale as part of its platform of services, and as your traffic increases, capacity is added instantly and on demand—there are no appliances to be sized, ordered, or shipped.

No industry is immune to security threats. And as more traffic is encrypted, inspecting that traffic has become mission-critical. A multilayered, defense-in-depth strategy that fully supports SSL inspection is essential to ensure that enterprises are protected from escalating threats hiding in their encrypted traffic.



Learn how **Zscaler** can inspect all of your SSL traffic without impacting performance or raising compliance concerns. Or, check your ability to inspect SSL/TLS traffic by using our **Internet Threat Exposure Analysis** tool.

About ThreatLabZ

ThreatLabZ is the security research arm of Zscaler. This world-class team is responsible for hunting new threats and ensuring that the thousands of organizations using the global Zscaler platform are always protected. In addition to malware research and behavioral analysis, team members are involved in the research and development of new prototype modules for advanced threat protection on the Zscaler platform, and regularly conduct internal security audits to ensure that Zscaler products and infrastructure meet security compliance standards. ThreatLabZ regularly publishes in-depth analyses of new and emerging threats on its portal, **research.zscaler.com**.

About Zscaler

Zscaler (NASDAQ: ZS) accelerates digital transformation so that customers can be more agile, efficient, resilient, and secure. The Zscaler Zero Trust Exchange™ protects thousands of customers from cyberattacks and data loss by securely connecting users, devices, and applications in any location. Distributed across more than 150 data centers globally, the SASE-based Zero Trust Exchange is the world's largest inline cloud security platform. Learn more at zscaler.com or follow us on Twitter **@zscaler**.

zscaler™