Defending Governments From Ransomware: Modernizing Malware Security with Cloud Sandboxing

A cloud-based solution enables governments to block fast-moving threats, close security gaps, and eliminate blind spots

zscaler™

The Colonial Pipeline ransomware attack in May 2021 not only cost $4.4M to rectify, it caused perceived gas shortages—and stockpiling—that significantly impacted millions of U.S. citizens.

While the Colonial Pipeline attack made news globally, there have been nearly 50 ransomware attacks on public sector organizations in the first six months of 2021. These attacks have cost millions, according to a Health and Human Services report released in June.

Combining downtime, people time, device and network cost, lost opportunity, and ransom paid, the average cost to rectify a ransomware attack for public sector institutions is substantial: education is $2.73M, healthcare is $1.27M, and local government is $1.64M.[1]

In 2020, ransomware attacks cost U.S. government organizations $18.88B.[2]

Ransomware and other data security threats are a serious concern for any organization. But the stakes are higher and the risks are greater for government agencies because they tend to store far more data than the private sector, and much of this data is extremely sensitive.

Agencies collect data on everything from income and investments to health conditions and criminal convictions. Citizens—who have no choice in giving their most private information to federal, state, and local agencies—understandably demand stronger information security from their government agencies. They also expect accountability from public officials when a data breach occurs. Therefore, high-profile cybercrime incidents can be career killers for CIOs and other government employees who are responsible for protecting sensitive information.

This paper discusses how public agencies must modernize their malware security solutions to cope with the growing ransomware threat and how a transformational security technology called cloud sandboxing can protect data from this 21st-century form of extortion.

[1] https://www.hhs.gov/sites/default/files/ransomware-trends-2021.pdf
[2] https://www.comparitech.com/blog/information-security/government-ransomware-attacks/

A Dynamic Response

Sandboxing isn't a new concept. Software developers have used sandboxes to test new programming code for many years. Cybersecurity professionals also use sandboxes to examine potentially malicious software. The process involves testing potential malware in an isolated environment where it can't impact production systems. This makes sandboxing a much more effective defense against fast-moving cyberattacks than traditional signature-based antivirus programs.

Signature-based solutions rely on known markers associated with viruses and malware to spot attacks. It's akin to matching a fingerprint or DNA sample to a known criminal. But new attacks slip by signature-based technology because the software simply can't find a match. Furthermore, hackers know how these programs work and have become more adept at getting around them. For instance, simply re-encoding a binary file is often sufficient to bypass a signature that was previously known.

Sandboxing overcomes these challenges by dynamically analyzing suspected malware in a safe environment. Rather than looking for known content within a given sample, it monitors the behavior of the sample when executed. This approach enables cloud sandboxing to address new attack vectors—even true zero-day threats (software vulnerabilities unknown to a vendor that hackers use to get into the system)—because it focuses on the outcome of the attack and observes malicious behaviors, which cannot be altered since they represent the goal of the attack.

Why cloud sandboxing is better

As hackers have become more sophisticated, malware and ransomware attacks have become harder to detect and stop. Cloud sandboxing addresses the elevated threat with the following capabilities:

Reach all locations: For any security control to be effective, it must have visibility into all your traffic, preferably inline. But to find the balance between cost and performance, organizations almost always put their sandbox appliances in the data center and set them to TAP mode, allowing potential malware to get through, opting to clean up the mess later. This approach can create huge security gaps, leaving networks open to compromise. The right cloud security solution closes these gaps by making the entire internet security stack, including sandboxing, accessible to all users no matter where they connect.

Inspect Secure Sockets Layer (SSL) traffic: SSL is meant to be secure, not easily intercepted or inspected. However, inspecting all traffic, including SSL traffic, is critical. Cloud sandboxing does this at scale without any impact on the user experience.

React to zero-day threats: Cloud sandboxing enables agencies to react quickly to emerging attacks. Threat intelligence is propagated globally within seconds, immediately protecting all users once a zero-day threat is identified. Cloud sandboxing allows organizations to easily scale protection against zero-day threats across all offices and all users with ease.

Analyze all file types: Standard sandbox solutions only conduct analysis on suspicious Windows executables and Windows libraries downloaded from suspicious URLs. A portion of the Windows executables and libraries are collected and run in a virtual environment to detect and block threats. However, an effective cloud sandboxing solution will analyze all supported files regardless of URL, including PDF, Java, Adobe Flash, APKs, archives (ZIP and RAR), Microsoft Office products, and 32-bit/64-bit Windows. Once a malicious file is detected, the technology will propagate fingerprints of that file throughout points within its cloud-based platform, effectively maintaining a real-time blacklist to prevent users anywhere in the world from downloading malicious files.

Building a Better Sandbox

Traditional sandboxes struggle to keep up in a mobile and cloud-based world. Until now, sandbox solutions have been physical appliances, which are expensive and cumbersome to implement. Like most organizations, government agencies employ remote staff and run satellite offices. But sandbox appliances must be deployed centrally, forcing agencies to implement costly backhaul network links to route all traffic to the headquarters or invest even more money to place appliances at every remote office.

Cloud sandboxing solves these challenges by implementing a new model for security–one that shifts access from a network-centric model to a policy-based approach. These solutions use a cloud security platform to provide policy-driven access to the internet and applications, delivering the highest level of security without the cost and complexity of hardware appliances.

Eliminating Blind Spots

Government agencies should look for cloud sandboxing solutions that are particularly effective at inspecting SSL-encrypted traffic, where a growing number of today's threats hide. Due to limits on processing power, SSL traffic often is ignored by sandbox appliances, opening a gaping security vulnerability due to the enormous growth in encrypted traffic. Google reports that, as of June 2019, 93 percent of all traffic across Google was encrypted.[3] As of April 2019, 78 percent of pages loaded by Firefox were encrypted.[4]

Cloud sandboxing uses the nearly unlimited processing power of the cloud to efficiently inspect SSL traffic without impacting end users. It does the same for traffic from content delivery networks, which is another growing threat vector. These networks serve web content to end users and are expected to carry 252 exabytes of traffic by 2022, up from 54 exabytes in 2017.[5]

While appliance technologies struggle to secure off-network users and lack the capability to deal with complex and sophisticated forms of malware, cloud sandboxing delivers full protection to users regardless of their location. These capabilities are vital for protecting sensitive citizen information as malware attacks become more dangerous. For instance, a seemingly harmless PDF file can contain the code to run scripts that download additional malware, which is then uploaded to a drop server and becomes undetectable to any desktop antivirus engine. That simple PDF file then can be downloaded over SSL, thereby preventing any detection unless you also scan SSL traffic. This enables hackers to encrypt data and assume control over your networks, leading to an eventual ransomware attack.

[3] https://transparencyreport.google.com/https/overview
[4] https://letsencrypt.org/stats/#percent-pageloads
[5] https://www.statista.com/statistics/267184/content-delivery-network-internet-traffic-worldwide/

Understanding the Ransomware Risk

Unfortunately, public sector systems may be particularly vulnerable to devastating malware attacks. The HHS Cybersecurity Program "Ransomware Trends 2021" released on June 3, 2021 reported that as of May 25, 2021, the organization had tracked 48 ransomware incidents targeting the United States Healthcare and Public Health sector since the beginning of the year. Ransomware attacks also target federal agencies.

Hackers target the public sector because many agencies and public institutions rely on legacy systems that haven't been updated to meet today's cybersecurity threats. Tight budgets and lack of resources can prevent government entities from modernizing security technology and seeking help from third-party experts to secure their data. At the same time, agencies are implementing more devices and technology platforms—from smartphones to mobile apps and tablets—giving hackers more points of entry into public sector networks.

Cloud-based security can help enable transformation across these areas by protecting data as agencies move toward mobile and cloud-based environments, and it enables them to do so without the cost and complexity of hardware-based security solutions.

CALL-TO-ACTION CHECKLIST: REDUCING YOUR RISK OF RANSOMWARE ATTACKS

Back up your data: This is the first and most important thing governments should do. In many recent cases of ransomware attacks, the victims refused to pay because they had backed up all their files and could restore their systems. Use an external drive or backup service to protect your organization's valuable data.

Educate employees: Many ransomware attacks occur when hackers exploit vulnerabilities in an organization's network, but they also can happen when an employee opens a suspicious file or accesses an internal network from a non-secure location. Governments need to implement training programs that educate employees about cybersecurity, the social engineering tactics hackers use, and ways to spot a suspicious file or an attempted malware attack.

Modernize your IT infrastructure: Legacy systems are ill-equipped to deal with today's cybersecurity challenges. Security as a service from the cloud helps you instantly protect all users on or off network, with minimal deployment costs. This should be a multifaceted effort that involves training for current IT staff; patching operating systems, firmware, and software on devices; recruiting more skilled talent; and leveraging third-party vendors to help your organization identify security holes and develop innovative, long-term strategies to resolve these issues.

Pay close attention to CDNs: Content delivery networks (CDNs) are themselves a bit of a threat vector. The reason is simple: nearly all security appliances assign a higher degree of trust to CDNs, such as Google and Akamai, as doing so protects their performance. Unfortunately, this implicit trust means content coming from these networks receives little or no inspection. Before hiring a cloud sandbox vendor, make sure its service vets and inspects CDN traffic and has tools in place to test security holes in your system as it relates to these networks.

Rely on a 360-degree approach: Seek a cloud sandboxing solution that inspects all your traffic—not just a fraction of it. Inspect encrypted traffic and set a goal to scan inbound and outbound SSL traffic, looking for malware and data leakage. This is the only way to reduce your risk of a malware attack or to isolate it before it infects all your systems.

To be effective, organizations must be able to analyze traffic regardless of employees' locations, the devices they use, or the protocols in place to access information. And all of this needs to be done without impacting performance for end users, which is where most appliance-based solutions fail. Hardware vendors will argue that more and larger boxes are required to handle the load, but this is a false equivalency since it does very little to enhance security. Today's security solutions need to leverage the power and scale of the cloud to provide policy-driven access to systems and applications wherever they are.

Conclusion

The world is changing and your IT security must change with it.

Most hackers are now sandbox-aware and are adept at creating countermeasures when launching a ransomware attack. Estimated ransomware damages cost the world more than $8 billion in 2018.[6] In 2020, that number was $20B.[7] This figure is likely to grow, making prevention even more critical for public sector organizations.

To address the threat, government agencies need security solutions that don't rely on signature-based anti-malware approaches that only inspect a portion of their traffic. Cloud sandboxing addresses fast-evolving malware threats, closes security gaps, and eliminates blind spots. Malware security that doesn't work for off-network traffic provides incomplete protection. Solutions that negatively impact the user experience or whose costs exceed its benefits are inadequate in today's digital workplace.

Public sector CIOs who want to combat malware attacks need sandboxing technologies that align with today's cybersecurity challenges. Effective cloud sandboxing solutions do their job regardless of the location or network the target is on—before malware infects computing devices. And if the malware does somehow evade the detection engine, a modern cloud sandbox solution can quickly detect and remediate that session before so much as a single packet makes it out.

In today's complex cybersecurity world, it's critical to move in this direction now. The long-term security of your data depends on it. And so do your citizens.

[6] https://cybersecurityventures.com/global-ransomware-damage-costs-predicted-to-exceed-8-billion-in-2018/
[7] https://features.propublica.org/ransomware/ransomware-attack-data-recovery-firms-paying-hackers/

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™

Zscaler, Inc.
110 Rose Orchard Way
San Jose, CA 95134
+1 408.533.0288
www.zscaler.com