Recon and Respond to Malware Threats in the Cloud

By Ravi Balupari and Abhinav Singh – ISSA member, Silicon Valley Chapter

The cloud is witnessing an exponential rate of adoption in enterprises, which is also becoming the new attack vector for delivering and propagating threats inside the networks. This article will cover some of the recent malware attacks seen in cloud infrastructures and what countermeasures can be adopted to defend against such threats.

Abstract

The cloud is witnessing an exponential rate of adoption in enterprises, which is also becoming the new attack vector for delivering and propagating threats inside the networks. This makes it essential for enterprises to build transparent security detection-and-response policies right from the beginning. This will ensure a stronger and more secure adoption of this infrastructure with better visibility and control over its usage. This article will cover some of the recent malware attacks seen in cloud infrastructures and what countermeasures can be adopted to defend against such threats.

Malware authorss have always been a step ahead in finding novel and innovative routes for infecting users, staying persistent, and moving laterally in the network. A quick glance at the last decade tells us that web drive-by and emails have been the biggest attack surfaces that were used in order to infect the users [6]. Considerable efforts were put up in building detection and prevention technologies against these attack vectors.

Recent trends show a shift towards the cloud as the next major attack surface [11]. As more and more critical data and infrastructure moves to the cloud, it will attract threat actors and advanced persistent adversaries in designing their attacks around the cloud. Figure 1 shows the distribution of malware types seen in a corporate cloud environment. It is essential for enterprises to design an effective detection-and-response model that can counter these threats. The cloud environment has several coherent properties that differentiate it from the traditional endpoint networked environment [5]. By carefully crafting an attack pattern, malware can exponentially enhance the attack surface in a cloud environment. We will discuss some of these use cases along with known malware attacks that can leverage cloud infrastructures to build an attack cycle.

The article is divided into two broad categories: 1) malware *delivered* through the cloud, and 2) malware *propagating* through cloud. The former explains the use of cloud infrastructures to host malicious files, while the latter explains the various mechanisms by which infections propagate through a cloud environment. We will also discuss effective use cases that can counter these threats in an enterprise environment.

Malware delivered through the cloud

Infection vector

There has been a significant increase in malware hosted on popular SaaS applications like Dropbox, Box, and Google

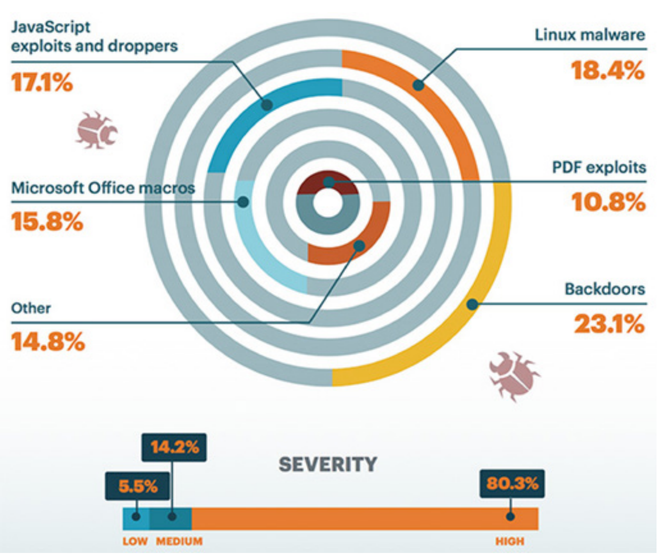


Figure 1 – Types of threats seen in the cloud [9]

Drive. Malware authors are increasingly using these cloud storage services to host their files, owing to the fact that these storage services might be whitelisted and/or the traffic is completely encrypted, thus blinding traditional security solutions. Once the file is uploaded to these cloud storage services, a sharable link is generated, which can be used in crafting various drive-by attack vectors. The link can now be weaponized by embedding it inside an Office file in the form of a macro, inside a .jar file as a next-stage payload download, inside a JavaScript script to drop the malware, or directly embedded in email sent to a targeted user. Once the first-stage attack is successful (execution of macro, .jar, or JavaScript), it will drop the next-stage payload (malware, spyware, banking Trojan, etc.) that may or may not be hosted over the same cloud storage application.

This is just a generic example as to how popular cloud storage services are exploited to deliver malware. According to the Netskope *Worldwide Cloud Report*, over 43 percent of malware found in enterprise cloud applications have delivered ransomware [8]. This itself gives us an idea of how prevalent malware threats are in a cloud environment. Not only ransomware, but also sophisticated banking Trojans are adapting to the cloud to bypass security measures. Telax, a spy banker Trojan campaign [2] targeting users in Brazil, was delivered through a URL shortening service and the Google cloud platform. Another banking Trojan, the CloudFanta malware campaign [12], was seen infecting user's through a popular Latin American SaaS application called Sugarsync. The SaaS application was used as a medium to host the malware payload. Another instance of an attack being delivered through the cloud is where phishing pages are hosted on cloud services; once it is loaded by the user, it is previewed directly in the browser, thus making it look less suspicious. If the user falls for the trap, he or she ends up with compromised credentials.

Another enterprise-based malware threat seen in an enterprise environment arises in case of cloud-based customer relations management (CRM) solutions. CRM solutions help enterprises to store and share customer data, delivered to corporate employees through the Web. Any employee using the CRM solution through his or her personal and infected device might transfer the infection to the CRM platform in the form of a file upload (we are assuming that the uploaded file is already infected/weaponized). This file now becomes a sitting time bomb. Once another employee downloads and executes the file, it will in turn infect his or her system. The attack methodology remains the same, but the addition of a cloud vector gives a new angle to the attack. It also gives attackers an upper edge as the entire traffic over SaaS appli-

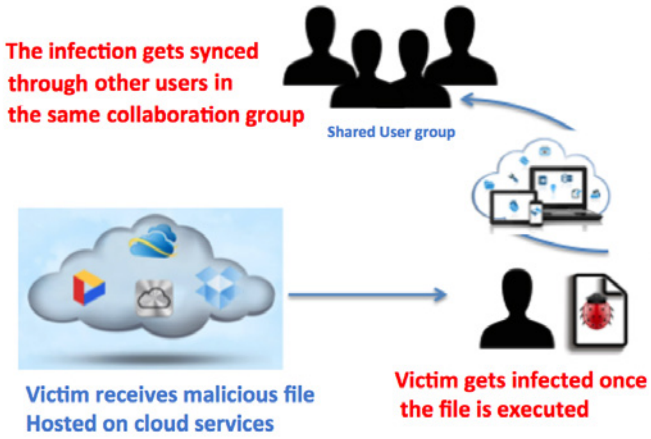

The infection gets synced through other users in the same collaboration group
Shared User group
Victim receives malicious file Hosted on cloud services
Victim gets infected once the file is executed

Figure 2 – Malware infection flowing through cloud applications and infecting users and the network

cations would be over HTTPS, thus blinding traditional security solutions like IDS, firewalls, etc. Figure 2 shows this process wherein a victim gets infected through a file hosted on a cloud environment (SaaS, CRM, etc). This infection in turn flows to other users within the same collaboration group by means of cloud syncing and sharing.

Responding to malware threats delivered through the cloud

The presence of encrypted traffic over the cloud leaves little option for building an effective detection-and-response solution using traditional security solutions. It is essential to understand that the cloud is an enterprise solution without boundaries. Employees would be accessing cloud applications from any part of the world using either an IT-managed or -unmanaged (personal) device, and file download/upload activity would be encrypted. Building a solution that can monitor and log any authorized or unauthorized files downloaded from cloud applications can be a good starting point. Also, using a threat-aware solution specifically designed for cloud-based applications can help in quickly identifying any suspicious malware action performed over a cloud-based sharing-and-collaboration environment. Identification of threats should be both in real time as well as an introspective mode that will also scan historical data for signs of infection.

Once the identification of threats is performed, the next challenge would be to identify the scope of the infection. In a cloud-based environment, files get shared and synced across all the users within the collaboration group. Identifying the point of origin of infection becomes critical in such scenarios. Collaborative environments like Office 365 and Salesforce possess advanced and complex sharing features, where it becomes critical to identify the origin of threats through solutions that can provide granular level details about activities performed by users in these environments. It is the responsibility of the system administrators to identify these use cases and assess it in their own corporate environment to make better judgments on cases resulting in mass infection or anomalies. Building a threat model based on auditing and vendor collaboration can also help in quickly remediating threats before becoming an epidemic.

Malware propagating through the cloud

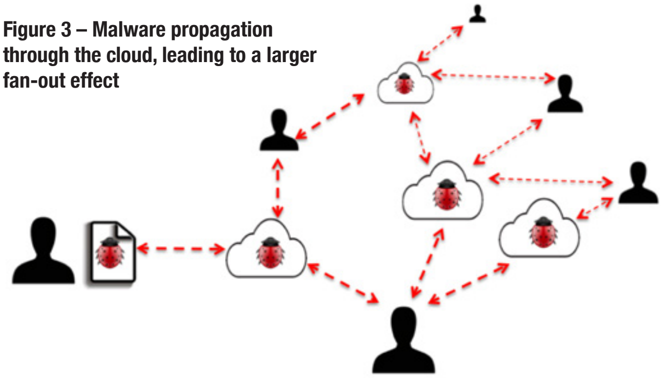
Infection vector

Now that we have built a background on how cloud services are used for delivering malware and other Internet-based threats, we will now try and build an understanding around how malware propagate through the cloud. The classic example is that of the Virlock family of ransomware [1]. Like any other ransomware, Virlock encrypts all the files it encounters on the infected machine. What is unique about Virlock is that it not only encrypts the files but also infects them. This makes Virlock a unique example of worm-propagation of ransomware. Consider two users, A and B, sharing the same cloud storage folder. Let us say user A gets infected with Virlock and the files located in his shared cloud folder get infected as well as encrypted. Now, since the files are updated, the SaaS application will go ahead and sync the updated files onto user B's desktop as well. If user B executes any of the files in the sync folder, her machine in turn gets infected with Virlock.

In a large enterprise environment there can be hundreds of users collaborating through the same syncing and storage folders. Threats such as Virlock lead to an elevated propagation of threats in a cloud environment, giving rise to a malware "fan-out" effect [7] where infection propagates from one user to every other user within the same collaboration group. There is, again, a possibility that the infection might go beyond the boundaries of controlled devices when the employee uses his or her personal device to access the cloud folder, thus infecting that device.

In case of personal or unmanaged devices, the infection can also flow inwards, where a pre-infected device might access the shared SaaS application. Under this scenario, the infected device might contain malware that can either replicate by copying itself to the mobile instance of the shared service

Figure 3 – Malware propagation through the cloud, leading to a larger fan-out effect



(Dropbox for mobile, Office 365 for mobile, etc.) or by infecting other files on the device, which later get shared through the Saas applications. Once this infected file replicates to the shared service, it gets transferred to every other user accessing the same folder (through automatic syncing of files across the user group). The actual malware might not exhibit the property of propagating through multi-platform devices, but the nature of cloud sharing and collaboration extends the threat landscape. Figure 3 depicts the effect of malware fan-out in a cloud-based environment. A recent cloud security report [10] suggests that in an enterprise cloud usage environment, over 55 percent of malware infected files found in cloud apps are shared amongst other users.

Another example of malware propagation through the cloud can be seen in cases where the cloud infrastructure is used by malware authors and APT groups in setting up their command and control infrastructure. This gives malware the ability to download more instructions about how it can further penetrate the attacked network. The benefit of hosting the command and control infrastructure over the cloud is the high uptime and availability, which is tough to receive with traditional web servers. It also gives them the flexibility to modify their computational resources based on requirement.

One of the prime examples of this is the highly sophisticated Inception Group [4]. This group conducted a mass espionage campaign targeting military officials, political diplomats, and business executives. The attack targeted popular mobile platforms including Android, iOS, blackberry, etc. The malware gathered a wealth of information from the infected targets: OS version, device name, username, group memberships, etc. All of this information is encrypted and sent to cloud storage via WebDAV. The framework is designed in such a way that all communications after malware infections such as configuration updates, malware updates, and data exfiltration can be performed via the cloud service.

Another similar but less sophisticated example of malware propagating through the cloud can be the case where the malware author uses an existing cloud infrastructure (IaaS) rather than setting up his own infrastructure from scratch. The Carbanak malware family [3] is an example of this category where it uses Google Docs for its command and control. Unlike the Inception Group it relies on an existing infrastructure to conduct its infection campaign.

Responding to the threats propagating through cloud

One of the biggest challenges to identifying malware propagating through cloud services is to distinguish between a legitimate cloud usage and a malicious one. The IT administrator should be capable of defining a clear policy to identify sanctioned cloud applications and block all unsanctioned applications. Identifying unsanctioned applications is not the complete solution for blocking malicious or unauthorized usage of cloud applications. There can be cases of insider threats where a personal instance of a sanctioned cloud application can be used to exfilterate data. For example, an organization can sanction Google Drive cloud applications, but they should ensure that users are not able to login to their personal instance of Google Drive and should only be able to login and use the corporate-sanctioned instance.

The next crucial point would be to identify authorized usage of sanctioned cloud applications to get granular-level clarity over user behavior and to enforce data loss prevention (DLP) policies. Such granular visibility over cloud traffic can also help in detecting anomalies by taking advantage of behavior analytics and machine learning to baseline a user's normal activities and detect anomalies in real time.

Threats such as ransomware can be countered by enabling file-version control in your cloud environment that can help in data recovery if the files get encrypted thorough these attacks. Regular backup of critical information becomes crucial in retrieving data that has been held hostage. Detecting worm-like self-propagation of malware in the cloud environment becomes critical in order to pin down the actual source of infection. The infection might begin from an email containing a malicious attachment or from an infected personal device connected to corporate network in a BYOD environment.

Towards an Open-Data Testbed for Self-Driving Vehicles

Continued from page 8

Ultimately, who gets to decide what are the important statistics and data to share? Who will be responsible to collect, verify, and ultimately report the data while protecting privacy? As we head towards a vehicular open-data test bed, there is one item for certain. The data must be privatized and secured before being stored in order to protect against privacy attacks and data breaches.

About the Author

Joshua Joy is a PhD candidate in Computer Science at UCLA, focusing on security and privacy in vehicular networks. He has developed scalable privacy mechanisms and is interested in data collection techniques enabling open-data platforms. Recent projects include the highly successful CrowdZen at UCLA, which is known as "Waze for the college campus." He may be reached at jjoy@cs.ucla.edu.

Once the origin of infection is determined, the incident response team can then perform forensic analysis on the endpoint to determine the actual cause of infection. A consolidated enterprise detection-and-response (EDR) integrated cloud-security solution can help in better tracking of these threats and can help in quickly remediating the threat across all the infected endpoints by running clean-up jobs through the EDR's agent.

Summary

The advancing migration of enterprise resources to a cloud-driven infrastructure is expanding the infrastructure horizons, thus posing a challenge for IT administrators and security analysts. Adapting to the new frontier of malware and virus attacks in these environments will be critical in protecting sensitive data. Predicting cyber attacks is as difficult as predicting an earthquake, but building an early-warning-and-detection system can reduce the damage significantly. It is very important for the organizations to build and adopt the right detection-and-prevention strategies right from the adoption stage of cloud-based infrastructures. This can enable building a stronger security and privacy base in a cloud-based, boundary-less environment.

References

1. Carlos, J., Chua, J., Fuentes, R. Virlock Combines File Infection and Ransomware, Trend Micro, March 2015 - http://blog.trendmicro.com/trendlabs-security-intelligence/virlock-combines-file-infection-and-ransomware/.
2. Desai, Deepen. New Spy Banker Trojan Telax Abusing Google Cloud Servers, Zscaler Blog, December 2015 - https://www.zscaler.com/blogs/research/new-spy-banker-trojan-telax-abusing-google-cloud-servers.
3. Diogos, T. Operation Grand Mars: A Comprehensive Profile of Carbanak Activity, SpiderLabs Blog, January 2017, Trustwave - https://www.trustwave.com/Resources/Spider-Labs-Blog/Operation-Grand-Mars--a-comprehensive-profile-of-Carbanak-activity-in-2016/17/.
4. Fagerland, S. and Grange, W. Blue Coat Exposes "The Inception Framework"; Very Sophisticated, Layered Malware Attack Targeted at Military, Diplomats, and Business Execs, December 2014 - https://www.bluecoat.com/security-blog/2014-12-09/blue-coat-exposes-“-inception-framework”-very-sophisticated-layered-malware.
5. GFI Software. On-Premise Vs. Cloud-Based Solutions, GFI Software – https://www.gfi.com/whitepapers/Hybrid_Technology.pdf.
6. Glassberg, Jason. What You Need to Know about "Drive-by" Cyber Attacks, Fox Business, February 2015, http://www.foxbusiness.com/features/2015/02/04/what-need-to-know-about-drive-by-cyber-attacks.html.
7. Netskope. Malware Attack Fan Out demo, Netskope - https://resources.netskope.com/h/i/214740060-netskope-demo-malware-attack-fan-out.
8. Netskope. Worldwide Cloud Report, Netskope Report, September 2016, slide 1/10 – https://resources.netskope.com/h/i/285921888-september-2016-worldwide-cloud-report.
9. Netskope. Worldwide Cloud Report, Netskope Report, September 2016, slide 4/10 – https://resources.netskope.com/h/i/285921888-september-2016-worldwide-cloud-report.
10. Netskope Press Release. Netskope Report Reveals 43.7% of Cloud-Based Malware Delivers Ransomware, September 2016 - https://www.netskope.com/press-releases/netskope-report-reveals-43-7-cloud-based-malware-delivers-ransomware/.
11. Panetta, Kasey. Is the Cloud Secure, Gartner blog, January 2017, http://www.gartner.com/smarterwithgartner/is-the-cloud-secure/.
12. Shapland, Rob. Why CloudFanta Malware Poses an Unusual Threat to Enterprises, SearchCloudSecurity, January 2017 - http://searchcloudsecurity.techtarget.com/tip/Why-CloudFanta-malware-poses-an-unusual-threat-to-enterprises.

About the Authors

Ravi Balupari is Director of Netskope Threat Research Labs, supervising the research of malware, ransomware, and other cloud security threats. Reach him at ravi.balupari@netskope.com.

Abhinav Singh is a security researcher whose core work areas include malware analysis, reverse engineering, threat research, and incident response. He is also the author of Metasploit Penetration Testing Cookbook *and* Instant Wireshark. *He may be reached at asingh@netskope.com.*