

Ransomware is costing companies millions. Could it cost you your job?

Cloud sandboxing protection is as essential to security as keys are to encryption. Preventing CIOs and CISOs from having to make excuses when it comes to APTs, zero-days, and ransomware.

✓ IMMUNITY FROM BEING A TARGET, BEING A VICTIM

There can be no doubt that every organization now requires advanced malware protection. Even so, there are plenty of organizations that have either not yet implemented this protection, or have it only somewhat implemented. Do these organizations recklessly believe they won't be targeted? Do they think their investment in a midrange sandboxing system will be sufficient protection, in spite of the fact that it can be easily bypassed? Or do they simply accept the risk and hope for the best?

Can the CIO and CISO honestly say they have immunized the business from these threats to the best of industry standards?

✓ EFFICACY IN THE REAL WORLD

Being effective at advanced security does not start and finish with a proof of concept and a purchase order for an appliance. It comes from executive leaders who make it clear that such threats have no place anywhere near their assets and can carry out that vision across all dimensions, including cost, locations, and user experience.

In other words, to be effective when it comes to advanced malware, the results must be real and measurable...at the speed of the business.

✓ BETTER BY DESIGN, PROVING IT WORKS

At some point, someone has to question why things, such as appliance-centric security models in a cloud-enabled world, just aren't working out—and then set out to fix what is broken. IT security executives who understand this know that their ability to stay off the hot seat directly correlates to their ability to find platforms that truly work. Equally important, they must adopt them ahead of their competitors, thereby saving time and money that their organizations could put to better use elsewhere.

If advanced malware security doesn't work for off-network traffic, it's simply bad design. If it works on the network but not with SSL-encrypted traffic, it's also bad design. And if it ruins the user experience or the cost exceeds the benefit, then that, too, is bad design. Getting the design right is what keeps a CIO and CISO from uncomfortable conversations in the boardroom and in the media.

Zscaler™ Cloud Sandboxing protection is for those who don't want to invest their pay raises in more appliances.

Analysts, security experts, and customers agree

“ This capability [advanced malware protection] is rapidly becoming a feature of a more-capable platform, not a stand-alone product or market. ”

– *Gartner Identifies the Top 10 Technologies for Information Security in 2014*



“ It seems a single day doesn't pass without some interesting new botnet emerging in the news...it's reassuring to know that Zscaler for APTs leverages the depth of its behavioral analysis with the breadth of its Security as a Service platform to deliver a uniquely comprehensive solution. ”

– *Tony Ferguson, IT Architect, Man Diesel & Turbo*



“ Accurate and consistent. Samples sent to the sandbox were properly classified and mitigated. Most efficient sandbox. Results were quick and the dashboard provided detailed forensic reporting. By design, block detect rate is better because only unknown samples are sent to the sandbox. ”

– *Miercom, Malware, Zero Day and Advanced Attack Protection Analysis*



STOPPING MALWARE: HOW CONFIDENT ARE YOU?

Let's start off with a simple challenge:

What if I gave you a link to a piece of new malware for you to hand your CIO, CISO, CFO, CEO—any of your company's c-suite executives or board members—and you asked them to click on it? Would you be reasonably confident that your defenses would quickly prevent the malware from downloading and executing? Seems simple enough, right?

As your organization's expert in information security, shouldn't the protections you've put in place be expected to handle something so fundamental? After all, this is really just a controlled test of something that is happening each and every day through phishing and other attack vectors.

Before you try and hit the straight pitch, consider some common curveballs about the malware:

- It is seemingly a simple PDF file, albeit containing the code to run scripts that download additional malware. The secondary payloads are specifically designed to seek out intellectual property and upload it to a drop server.
- The file, along with the secondary payloads, will be hosted on a CDN (content delivery network). More on why that matters a bit later.
- The file, along with the secondary payloads, is currently undetectable by any desktop antivirus engines (just validated by running through VirusTotal).
- It will be downloaded over SSL, thereby preventing any detection unless you are scanning SSL traffic.
- You will encourage the executives or board members to download it when they are on the network, as well as while traveling and/or at home (completely off the corporate network).

“After deploying Zscaler, we've seen a 100X reduction in malware detected by our downstream security infrastructure.”

— **Christopher Hudel**, Chief Information Security Officer, SPX Corporation

DID YOU KNOW?...

- By the end of 2016, SSL is expected to consume 60% of all web traffic (NSS Labs), yet very few non-Zscaler organizations inspect SSL traffic.
- Inspecting SSL traffic can require as many as 8X the number of security appliances.
- CDNs are the source of over 40% of web traffic—Akamai alone claims as much as 30% of that.
- Gartner dropped their antivirus magic quadrant analysis way back in 2006, indicative of what security practitioners know all too well: real security requires much more.

So right about now you are quite possibly thinking, “This is what our ridiculously expensive sandbox appliance is for!” And yet, you don’t let your boss click on that link because you have grave concerns. Why? Don’t you trust that your chosen solution for detecting unknown malware—which is absolutely what we are talking about here—can detect and then block the malware?

After all, it’s the promise of sandboxing to do the job, regardless of the location or network our target is on, before the malware ends up on the computing devices. Or, if the malware does somehow evade the detection engine, the sandbox should quickly detect and remediate that session before so much as a single packet makes it out. That’s what it’s there for, right?

Well, not so fast...

This scenario highlights the limitations of appliance-based sandboxing products in the more modern cloud era. Specifically, there are a few realities that bring us to this point:

- **Blind Spots:** Appliances are physical—even those running as virtual appliances are running on physical hardware—and have to be located somewhere, leaving you to force the traffic through them if they are to be at all effective. Remote offices and employees are often only protected by a subset of what exists at the larger offices, which is especially true for APT protection.
- **Encryption:** Further adding to the blind spots, but in its own category and deserving special attention, SSL inspection is seldom enabled, even when appliances are used. Cost, complexity, performance, and limited visibility are typically cited as the reasons for this omission by design.
- **Scale:** Scalability becomes a challenge as appliances, unlike a comprehensive cloud platform like Zscaler, end up receiving all files, absent and filtering of known bad files before they ever hit the sandbox. This is great for appliance vendors as they get to sell you even more and larger appliances, further depleting your IT budget and limiting your ability to improve in other critical areas.
- **Compromise:** In order to find the balance between cost and performance, enterprises almost always put their sandbox appliances in tap mode, intentionally letting things get through with the goal of cleaning up the mess later. So, even if you believe that the best approach is to actually defend your network from zero-day and advanced exploits, you are compromised by the rules the appliance vendors have set up to sell more hardware capacity. It just doesn’t add up.

SANDBOXING: NOT REALLY ALL THAT NEW

The term “sandbox” is nothing new. Information security professionals have been using some form of sandboxing for decades. The term conveys the idea of testing something in a secured lab setting where it can’t impact production systems. More recently, the term has been applied more specifically to physical objects (appliances) as a way to market them for fighting against the latest threat vector (APTs).

What preceded all of the clever marketing and packaging of today’s sandboxes are several programs, many of which are still very much alive in one way or another, serving as the basis for the more contemporary commercial offerings. The more popular ones are known as Anubis, QEMU, and Libvert, and those interested in digging deeper would do well to research these themselves. Which is exactly what hackers do when trying to come up with ways to get around the various APT defenses.

CONNECTING THE DOTS WITH CLOUD SANDBOXING

1 What is cloud sandboxing?

Cloud sandboxing is a dynamic analysis technique designed to identify malware that doesn't rely on the use of signatures. It is a technique that has been leveraged by the research community for some time and is now seen as a critical component of a defense-in-depth strategy due to increasingly complex attacks that are simply not identified by traditional signature-based approaches.

Cloud Sandboxing takes a fundamentally different approach. Rather than looking for known content within a given sample, it instead relies on monitoring the behavior of the sample when executed. In this way, when a new attack vector is exploited, even when dealing with a true zero-day, malware can still be flagged as malicious based not on the exploited vulnerability but rather on the behaviors exhibited.

2 Why is cloud sandboxing analysis needed?

Simple. Because static, signature-based methods just don't get the job done:

- URL filtering fails because malware can be hosted anywhere and is commonly hosted at "legitimate" sites as opposed to attacker-controlled domains. Getting past these controls is now a trivial task.
- Antivirus, being signature-based, is ineffective against new attacks. The software simply can't find a match. It's like trying to match a fingerprint or DNA sample to a criminal who has never before had his/her data recorded. To make matters worse, simply re-encoding a binary file is often sufficient to bypass a signature that was previously known. As with URL filtering, the criminal has the upper hand here, not you. To be clear, AV is ineffective against new attacks.

In contrast, BA focuses on the outcome of the attack, the malicious behaviors ultimately observed, which cannot be altered as they represent the goal of the attack.

3 Why are appliances so limited?

Between remote employees, satellite offices, and SSL-encrypted traffic, organizations that have made significant investments in appliance-based solutions quickly realize that only a fraction of their overall traffic is being inspected. And because visibility is critical in security, all traffic must be inspected, regardless of the source or delivery mechanism. In order to be effective, we must be able to analyze binaries regardless of employees' location, the devices they are using, or the protocols being used to access information.

- ▶ And of course all of this needs to be done without any performance issues as seen by the users. This is where appliance vendors fail, as they will simply argue that more and larger boxes are required to handle the load.

YOU ZIG, THEY ZAG: BECAUSE THAT'S JUST HOW THE GAME IS PLAYED

Even with the latest sandboxing techniques, the more advanced the threat, the less likely you are to be able to detect it coming in. But there are some protections you must have in place if you hope to try to stop attacks.

For example, this discussion assumes you are addressing SSL inspection as well as ensuring that you are seeing all the traffic you should, both on and off the corporate network. If you haven't reached that level just yet, then this piece, while interesting, will probably not serve your desired outcomes. As the saying goes, you will be putting the cart before the horse.

Having addressed SSL inspection and the right level of visibility, let's say your sandbox is now getting all the interesting files. Why is it that some of the more advanced threats are still evading your defenses and getting through? And what can be done to mitigate each? The list of evasion techniques is actually quite long and evolving over time, so we'll just highlight some common techniques to illustrate the fact that sandbox appliances, absent the full picture of what is really going on, are increasingly mismatched against their counterparts.

As we know, a sandbox is really just pretending to be a user's PC, and it has to be better at pretending than the malware is at detecting the ruse. It sounds simple enough, but it hardly is. If you can imagine all the clever ways you might go about determining how to detect if you are running in a sandbox, you can bet the elite hacker community has had the same thoughts.

👉 Content delivery networks will carry over half of Internet traffic by 2019. Globally, sixty-two percent of all Internet traffic will cross content delivery networks by 2019 globally, up from 39 percent in 2014. 🗨

— *Cisco Visual Networking Index: Forecast and Methodology, 2014–2019 White Paper*

HOW A SANDBOX CAN BE IDENTIFIED (AND, SOMETIMES, BYPASSED):

- **VM/CPU detection:** Simply look for processes, registry keys, and other tell-tale signs that this is a virtual machine instance of a popular operating system rather than a standard desktop install. If it doesn't quite add up, just don't execute the malicious parts of your code, also known as Dynamic Code Execution, while in this state.
- **Timers:** As users won't tolerate waiting terribly long for files to be delivered, malware could simply come with a timer that prevents it from executing for, say, five to 10 minutes after it is launched. It's a simple but effective technique. Most sandboxes will, of course, deploy their own countermeasure, which is to adjust the clock in order to fool the malware into thinking the required time has lapsed. But in increasingly advanced attacks, this can also be detected and worked around.
- **Testing:** Once the hacker thinks the build is about right, testing is done to gain some degree of confidence that it won't be discovered. And this is not testing against your infrastructure, but rather in their own test sandboxes. If the budget is low, then the aggressor might just be running it through sites such as Anubis and VirusTotal. But if the budget is big, such as with a state-sponsored attack, you can bet they have many, if not all, of the same appliances you run to test against. When it comes up clean, it's time to target your users to go straight through your defenses.
- **Content delivery networks (CDNs):** What most don't realize about CDNs is that they, themselves, are a bit of a threat vector. The reason is simple: nearly all security appliances provide a higher degree of trust to CDNs, such as Google and Akamai, as doing so protects their performance (marketing data sheet numbers). Unfortunately, this implicit trust means things will get through with little to no inspection. And let's face it, it's hard to enforce a zero-trust security model when your appliance vendors are trusting huge swaths of Internet traffic for you and in spite of the security policy you think you implemented. In fact, when you run the Zscaler Security Preview tool, this is one of the clever ways we are able to demonstrate bypassing your security controls—safely, of course.

HERE'S WHAT IT TAKES TO KEEP MALWARE FROM REACHING THE DESKTOP, NETWORKS:



Reaching all locations

In order for any security control to be effective, it must have visibility into all the traffic, preferably inline and able to block bad traffic vs. those that are in tap mode and only able to alert after the malware has hit its target. It seems so simple and obvious, but the gaps faced by organizations are often huge. Zscaler closes the gaps by making the entire Internet security stack universally accessible.



Seeing inside the SSL blind spot

SSL traffic is already approaching 50% percent of total web traffic, and is expected to grow to 60 percent by the end of 2016. And as we all know, SSL is meant to be secure, not easily intercepted nor inspected. But inspecting all traffic, including SSL traffic, is what Zscaler does—at scale and without an impact to the user experience.

Most large enterprise customers running Zscaler have already implemented SSL inspection with great results. And none of them ever had to size up a bunch of appliances or compromise on what traffic gets inspected. It all does.

“There are known knowns. These are things we know that we know. There are known unknowns. That is to say, there are things that we know we don't know. But there are also unknown unknowns. There are things we don't know we don't know.”

– Donald Rumsfeld

STANDARD CLOUD SANDBOX

Zscaler conducts sandboxing 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.

ADVANCED CLOUD SANDBOX

Zscaler conducts sandboxing analysis for all supported files, regardless of URL:

- PDF
- Java
- Adobe Flash
- sAPKs Android Application Packages
- Archive: ZIP, RAR
- Microsoft Office: Word, Excel, Powerpoint
- 32 bit/64 bit Windows executables and DLLs

Once Zscaler detects malicious files, it propagates fingerprints of malicious files to all Zscaler Enforcement Nodes (ZENs) throughout the cloud, effectively maintaining a real-time blacklist to prevent users anywhere in the world from downloading malicious files.

ZSCALER HAS CRACKED THE CODE ON ADVANCED MALWARE: THE RIGHT PROCESS



Pre-Filtering

Security appliance vendors have no little to no incentive/capability to do this for you!

In-line Antivirus
Blacklisting: 40 threat feeds
Signature-based Modules

Security appliance vendors have no little to no incentive/capability to do this for you! There's really no point in scanning something that is already known to be bad, right? By filtering out as much of these files (again, globally and even within SSL encrypted traffic), we are able to take all the knowledge that comes from over 15 million users and 40 threat feeds to really speed things along.



Suspect Pre-Processing through Static Analysis

Multi-AV Scanner
Heuristics Signatures
Packer Detection
Whitelisting
Fuzzy Hashing

At this point we suspect something might not be quite right, or at the very least we just don't have enough to rule out whether or not the binary is innocent, so we will pre-process it just to be sure. A file that we have no hash for and is clearly the first time it has been seen in the cloud is going to get this special attention. This is very efficient, as it best filters the known good and bad.



Going Deep with Full Dynamic Cloud Sandboxing

Execute and Monitor
Flagging Malicious Activity
Flagging Suspicious Activity

It's finally time for "sandboxing". Fully inline and exceeding the capabilities of dedicated appliances, the engine goes to work, fully aware that the bad guys are "sandbox aware" and quite clever at their own countermeasures, the cloud-based engines are always kept up to date, with more than a few tricks of their own up their sleeves.



Even more – Final Pass of Static Analysis and Reporting

All Static Scans...Again!
Highly Detailed Reporting

This is same as static analysis but it runs on all the samples/artifacts that are collected from the sandbox virtual machine at the end of dynamic analysis phase. All of this is then captured in the final report.



The World Comes Together!

Share with over 15M Users
Over 15M Users Share Back
Entire Global Cloud Updated

There's no imagining the possible here. It's real. As others find and clean up traffic, you get the benefit and share back yourself.

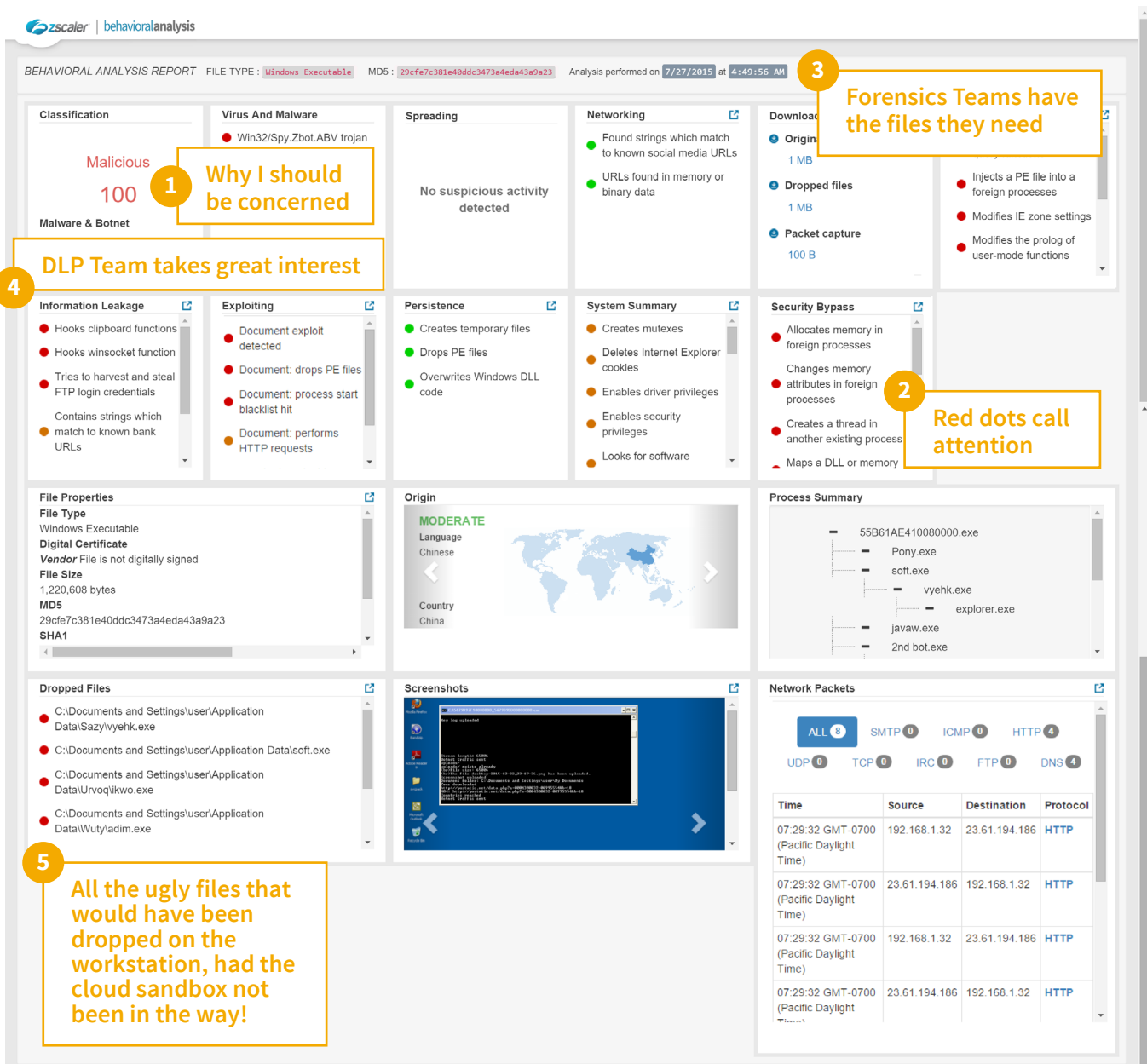
“ You may say I'm a dreamer, but I'm not the only one. I hope some day you'll join us, as the world will live as one. ”

– John Lennon

DETAILED ANALYSIS—THE LIFEblood OF A TRUE SECURITY PROFESSIONAL.

Having seen a malware alert in your SIEM that has piqued your interest, you can simply click the shortcut to access the detailed BA report. Here, you will see everything your professional needs require. Some will merely be events, while others may be part of a broader incident response. In either case, the information needed in the moment is there for immediate investigation.

What's really great here is that you won't be wasting your time looking through problems that have already been solved, as the only files sent to the cloud sandboxing engine are those that are truly the new unknowns.



BEHAVIORAL ANALYSIS REPORT FILE TYPE: **Windows Executable** MD5: **29cfe7c381e40ddc3473a4eda43a9a23** Analysis performed on **7/27/2015** at **4:49:56 AM**

Classification
Malicious
100
Malware & Botnet

Virus And Malware
 ● Win32/Spy.Zbot.ABV trojan

Spreading
 No suspicious activity detected

Networking
 ● Found strings which match to known social media URLs
 ● URLs found in memory or binary data

Downloads
 ● Origin 1 MB
 ● Dropped files 1 MB
 ● Packet capture 100 B

3 Forensics Teams have the files they need

1 Why I should be concerned

4 DLP Team takes great interest

2 Red dots call attention

5 All the ugly files that would have been dropped on the workstation, had the cloud sandbox not been in the way!

Information Leakage
 ● Hooks clipboard functions
 ● Hooks winsocket function
 ● Tries to harvest and steal FTP login credentials
 ● Contains strings which match to known bank URLs

Exploiting
 ● Document exploit detected
 ● Document: drops PE files
 ● Document: process start blacklist hit
 ● Document: performs HTTP requests

Persistence
 ● Creates temporary files
 ● Drops PE files
 ● Overwrites Windows DLL code

System Summary
 ● Creates mutexes
 ● Deletes Internet Explorer cookies
 ● Enables driver privileges
 ● Enables security privileges
 ● Looks for software

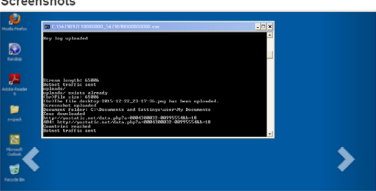
Security Bypass
 ● Allocates memory in foreign processes
 ● Changes memory attributes in foreign processes
 ● Creates a thread in another existing process
 ● Maps a DLL or memory

File Properties
 File Type: Windows Executable
 Digital Certificate: Vendor File is not digitally signed
 File Size: 1,220,608 bytes
 MD5: 29cfe7c381e40ddc3473a4eda43a9a23
 SHA1: [redacted]

Origin
 MODERATE
 Language: Chinese
 Country: China

Process Summary
 55B61AE410080000.exe
 - Pony.exe
 - soft.exe
 - vyehek.exe
 - explorer.exe
 - javaw.exe
 - 2nd bot.exe

Dropped Files
 ● C:\Documents and Settings\user\Application Data\Sazy\vyehek.exe
 ● C:\Documents and Settings\user\Application Data\soft.exe
 ● C:\Documents and Settings\user\Application Data\Urvqikwo.exe
 ● C:\Documents and Settings\user\Application Data\Wuty\adim.exe

Screenshots


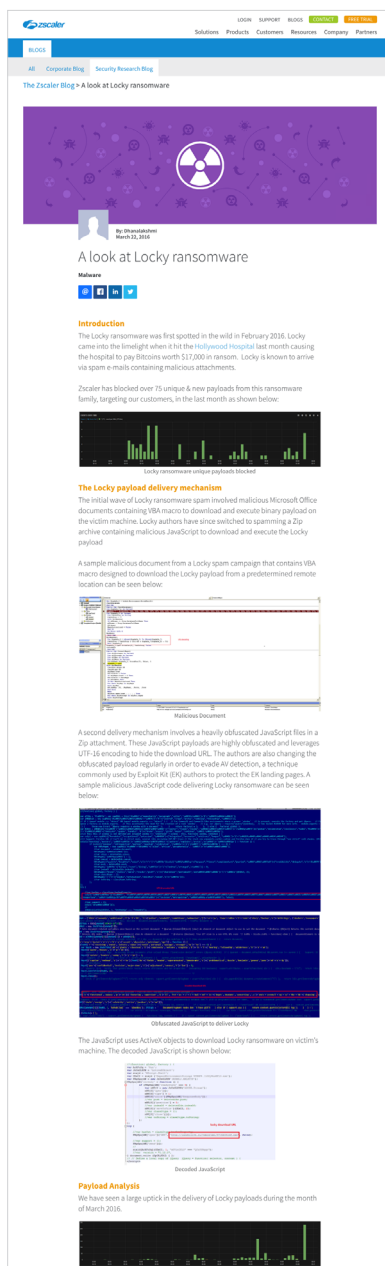
Network Packets

Time	Source	Destination	Protocol
07:29:32 GMT-0700 (Pacific Daylight Time)	192.168.1.32	23.61.194.186	HTTP
07:29:32 GMT-0700 (Pacific Daylight Time)	23.61.194.186	192.168.1.32	HTTP
07:29:32 GMT-0700 (Pacific Daylight Time)	192.168.1.32	23.61.194.186	HTTP
07:29:32 GMT-0700 (Pacific Daylight Time)	23.61.194.186	192.168.1.32	HTTP

THREATLABZ—WHEN ANALYSIS HAS TO GET REALLY, REALLY, REALLY DEEP.

There will be times where, even though Zscaler has prevented the zero-day malware from landing on any of your systems, even deeper analysis is needed. Of course this is often driven by the media, but there are certainly other situations out there that may capture your attention.

This is where ThreatLabZ comes in. As a premier security research team, constantly on the lookout for emerging threats, the team's analysis is posted in the public domain for all to see. So whenever someone asks about the latest ransomware or other exploit of immediate interest, the **ThreatLabZ site** is a great place to explore and learn.



Introduction

The Locky ransomware was first spotted in the wild in February 2016. Locky came into the limelight when it hit the Hollywood Hospital last month causing the hospital to pay Bitcoins worth \$17,000 in ransom. Locky is known to arrive via spam e-mails containing malicious attachments.

Zscaler has blocked over 75 unique & new payloads from this ransomware family, targeting our customers, in the last month as shown below:

The Locky payload delivery mechanism

The initial wave of Locky ransomware spam involved malicious Microsoft Office documents containing VBA macros to download and execute binary payload on the victim machine. Locky authors have since switched to spamming a Zip archive containing malicious JavaScript code to download and execute the Locky payload.

A sample malicious document from a Locky spam campaign that contains VBA macros designed to download the Locky payload from a predetermined remote location can be seen below:

A second delivery mechanism involves a heavily obfuscated JavaScript file in a Zip attachment. These JavaScript payloads are highly obfuscated and leverages UTF-16 encoding to hide the download URL. The authors are also changing the obfuscated payload regularly in order to evade AV detection, a technique commonly used by Exploit Kit (EK) authors to protect the EK landing pages. A sample malicious JavaScript code delivering Locky ransomware can be seen below:

Obfuscated JavaScript to deliver Locky

The JavaScript uses ActiveX objects to download Locky ransomware on victim's machine. The decoded JavaScript is shown below:

Decoded JavaScript

Payload Analysis

We have seen a large uptick in the delivery of Locky payloads during the month of March 2016:

We looked at one of the newer Locky variant that was seen in the wild recently. The analyzed Locky payload is a 32-bit Microsoft Visual C++ compiled Windows executable packed using custom packer routine.

Upon execution, the malware first checks for the user & system default language preferences of the infected system and terminates itself if the language is Russian. Locky creates a copy of itself as "ntemp\lvchost.exe" and an auto start registry key entry to ensure persistence upon system reboot. In order to mask a successful infection on the system, Locky creates the following registry keys with value name "pubkey" and "paytext" as seen below:

Locky registry key

"pubkey" is used to store the RSA key used for encryption
 "paytext" is used to store the payment related information

Upon successful infection, Locky will encrypt the following file types on the victim machine:

File types encrypted

These encrypted files are renamed to unique ID generated for the victim's machine followed by unique file ID and a "Locky" extension. The ransom note is displayed in a bitmap image that is also set as a wallpaper for the infected user's desktop as seen below:

Ransom note

As open 15 cases of other crypto ransomware families, victim's files are held as hostage for a ransom. The ransom payment instructions for recovering the private RSA key required to decrypt the user files is readily available through the URLs mentioned in the ransom note:

Payment instructions

Command & Control communication

The Locky payload contains a list of hardcoded Command & Control (C&C) server IP addresses that appear in plain text in the unpacked binary as seen below:

Hardcoded C&C IPs

In addition, Locky ransomware also leverages a custom Domain Generation Algorithm (DGA) for hiding its C&C server location. The DGA algorithm used for generating possible C&C domains in the payload that we analyzed can be seen below:

Domain Generation Algorithm

Locky communicates with the C&C server using custom encryption and the following HTTP request format:

POST http://[hardcoded IP or DGA domain]/main.php

Sample encrypted C&C communication

The initial C&C communication typically consists of three HTTP POST requests.

Request #1: Register the infected system's unique ID and request RSA key to be used for encrypting user files. The figure below shows the content of this POST request in plain text:

Request #2: Request the content of ransom note to be displayed on the infected system asking for payment. Below is the content of this POST request as well as the response from the C&C server in decoded form:

Request #3: The final request sends the statistics about successfully encrypted files as seen below:

Hardcoded C&C IPs

In addition, Locky ransomware also leverages a custom Domain Generation Algorithm (DGA) for hiding its C&C server location. The DGA algorithm used for generating possible C&C domains in the payload that we analyzed can be seen below:

Domain Generation Algorithm

Locky communicates with the C&C server using custom encryption and the following HTTP request format:

POST http://[hardcoded IP or DGA domain]/main.php

Sample encrypted C&C communication

The initial C&C communication typically consists of three HTTP POST requests.

Request #1: Register the infected system's unique ID and request RSA key to be used for encrypting user files. The figure below shows the content of this POST request in plain text:

Request #2: Request the content of ransom note to be displayed on the infected system asking for payment. Below is the content of this POST request as well as the response from the C&C server in decoded form:

Request #3: The final request sends the statistics about successfully encrypted files as seen below:

Conclusion

Locky is the latest addition to Ransomware, one of the most active & lucrative malware strains seen in past three years. This new ransomware family follows the same model of using asymmetric (public key) encryption to lock user documents and demand ransom for the decryption key. The delivery vector has been primarily spammed e-mail attachments that are responsible for downloading the Locky payload. We also noticed an interesting overlap in the recent campaigns where same URLs were being used to deliver both Dridex & Locky payloads.

Zscaler's ThreatLabZ has confirmed coverage for the initial downloader and Locky payloads, ensuring protection for organizations using Zscaler's Internet security platform.

Research by: Deepen Desai, Dhanalakshmi PK

CALL TO ACTION CHECKLIST

- ✓ **Be bold:** Know with relative certainty that top executives in the company can click on a phishing email and that your security protection will sufficiently block the attack, even if they are the very first to encounter it.
- ✓ **Run Security Preview:** Test your current security at <http://securitypreview.zscaler.com>, both while on the organization network as well as while remote. Are the results acceptable to the business leadership? While here, also subscribe to ThreatLabZ updates!
- ✓ **Inspect encrypted traffic:** Set a goal to scan outbound SSL traffic, looking for malware and data leakage. Don't let another quarter pass without having this in place.
- ✓ **Play offense—globally:** Leverage the power of the cloud, changing the rules of the game from simple defense to all-out offense. If a user clear across the globe encounters the newest malware for the first time (patient zero), you need that protection within minutes. Likewise, you want to share what you have learned.
- ✓ **Take the trash out:** If you are eating a meal but the food is spoiled, it is doubtful you would continue. Yet that's akin to what businesses do all the time, saying that their capital assets (software and hardware) must first be depreciated. That's just not good for the health of the business though. If what you have is not good, by all means, make the simple case to throw it out!

“ As long as everything is routed through Zscaler, from a security perspective, I'm happy. ”

– **John Taylor**, Global Head of IT Security and Service Continuity, British American Tobacco

“ 54 % of the advanced threats we see are over SSL. ”






– **ThreatLabZ Research (2015)**, Zscaler

CONTACT US

Zscaler, Inc.
110 Rose Orchard Way
San Jose, CA 95134, USA
+1 408.533.0288
+1 866.902.7811

www.zscaler.com

FOLLOW US

 facebook.com/zscaler
 linkedin.com/company/zscaler
 twitter.com/zscaler
 youtube.com/zscaler
 blog.zscaler.com



Zscaler™, SHIFT™, Direct-to-Cloud™ and ZPA™ are trademarks or registered trademarks of Zscaler, Inc. in the United States and/or other countries. All other trademarks are the property of their respective owners. This product may be subject to one or more U.S. or non-U.S. patents listed at www.zscaler.com/patents

©2017 Zscaler, Inc. All rights reserved. Z170329