CLOUDPIERCER
BYPASSING CLOUD-BASED SECURITY PROVIDERS
AGENDA

CLOUD SECURITY
What is cloud-based security?

VULNERABILITIES
How can cloud security be bypassed?

DEFENSES
How can we prevent these vulnerabilities?

ONLINE TOOL
Discover our online tool to scan for vulnerabilities

cloudpiercer.org
Thomas Vissers, Tom Van Goethem, Wouter Joosen, Nick Nikiforakis
CLOUD SECURITY

What are cloud-based security providers (CBSPs)?
CLOUD-BASED SECURITY

DDoS attacks

- Flooding web servers with loads of traffic to take it down
  - Volumetric attacks
  - Application-level attacks

- Classic on-premises security devices are usually ineffective
  - Network connections saturate

- Attacks become ever larger and more common
CLOUD-BASED SECURITY PROVIDERS

DDoS attacks – Larger

Survey Peak Attack Size Year Over Year

Image from Arbor Networks

cloudpiercer.org

Thomas Vissers, Tom Van Goethem, Wouter Joosen, Nick Nikiforakis
CLOUD-BASED SECURITY PROVIDERS

DDoS attacks – more common

- A plethora of DDoS-as-a-service providers ("stressers" or "booters")
  - DDoS attack at the click of a button
  - Very cheap (in line with their quality)

<table>
<thead>
<tr>
<th></th>
<th>Bronze</th>
<th>Platinum</th>
<th>Crystal</th>
<th>VIP</th>
</tr>
</thead>
<tbody>
<tr>
<td>Attack Methods</td>
<td>15+</td>
<td>40+</td>
<td>50+</td>
<td>60+</td>
</tr>
<tr>
<td>Attacks per hour</td>
<td>10</td>
<td>30</td>
<td>75</td>
<td>Unlimited</td>
</tr>
<tr>
<td>Gbps TN</td>
<td>180</td>
<td>180</td>
<td>180</td>
<td>300</td>
</tr>
<tr>
<td>VIP</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>VIP</td>
</tr>
</tbody>
</table>

cloudpiercer.org

Thomas Vissers, Tom Van Goethem, Wouter Joosen, Nick Nikiforakis
Also about... Web application attacks

- SQL injections, XSS, ...

*OWASP TOP10*

- WAF: Often rules and signatures are used to detect attacks

*Distinguishing between benign and malicious web request is a complex and delicate process*
CBSPs reroute and filter the customers’ traffic through their cloud

> CBSP forwards clean traffic to customer’s server
Cloud-based security: several flavors

- DNS vs. BGP rerouting to scrubbing centers
  
  BGP requires a Class C network infrastructure (/24 IP range)

- On-demand vs. always-on
  
  On-demand requires in-house expertise or CPE to decide when to flick the switch

- Other types
  
  On-premises, hybrid protection, DDoS protection by ISPs (Clean Pipes), ...
Cloud-based security: several flavors

- **DNS** vs. BGP rerouting to scrubbing centers
  
  *BGP requires a Class C network infrastructure (/24 IP range)*

- On-demand vs. **always-on**
  
  *On-demand requires in-house expertise or CPE to decide when to flick the switch*

**Popular solution**

10% of top 10,000 websites use DNS-rerouting, always-on cloud security services

Cloud security was a $4.5 Billion market in 2015 – by 2020, $12 billion market
CLOUD-BASED SECURITY

Always-on + DNS...? What are these services?

- Often a combination of CDN + Security services
  
  The geographically distributed nature of CDNs is ideal for high-absorbing scrubbing centers

- “DDoS protection for the masses”
  
  > No infrastructural requirements
  > No expertise needed
  > Quick and easy installation (change DNS records)
  > Low cost (sometimes free)
CBSPs reroute and filter the customers’ traffic through their cloud

> Customer’s domain name resolves to CBSP’s infrastructure
> CBSP forwards clean traffic to customer’s server (=origin’s IP address)
CLOUD-BASED SECURITY PITFALL

“DIRECT-TO-IP ATTACKS”

> Origin’s IP address should be kept secret
> Exposure of the IP address jeopardizes the entire security mechanism

cloudpiercer.org
Thomas Vissers, Tom Van Goethem, Wouter Joosen, Nick Nikiforakis
LARGE-SCALE ANALYSIS

1. Sampled ~18,000 domains using always-on DNS-based cloud security

2. Tested for 8 potential origin IP leaks on each of them

3. Subjected all candidate origin IP addresses to a verification test
   > Filtered out IP addresses belonging to CBSPs
   > Retrieve home page via CBSP
   > Retrieve home page via candidate IP address
   > If both return the same page, the candidate IP address is an origin
LARGE-SCALE ANALYSIS

our large-scale evaluation of 18,000 CBSP protected domains reveals that 7 of 10 websites are exposed through at least one vulnerability.

cloudpiercer.org
Thomas Vissers, Tom Van Goethem, Wouter Joosen, Nick Nikiforakis
VULNERABILITIES

How can the server’s IP address be exposed?
VULNERABILITY 1: SUBDOMAINS

- CBSPs rely on HTTP “Host” header to forward requests
  Breaks non-host header protocols (FTP, SSH, ...)
  ssh root@domain.com now connects to the CBSP without any notion of the domain
  ssh root@104.131.120.106 must be used

- “Let’s just use a direct-to-origin subdomain for SSH!”
VULNERABILITY 1: SUBDOMAINS

Our findings

- Scanned 5,000 subdomains per domain
  
  Verified each IP address to which they resolved

- 43% of domains had a direct-to-origin “backdoor”

  - ftp.example.com (3,952 domains)
  - direct.example.com (3,583 domains)
  - mail.example.com (3,203 domains)
  - ...

cloudpiercer.org
Thomas Vissers, Tom Van Goethem, Wouter Joosen, Nick Nikiforakis
VULNERABILITY 2: DNS RECORDS

- Other DNS records might still reveal your origin

- Example – SPF records
  
  "v=spf1 ip4:104.237.146.167 -all"
  
  *TXT record that allows you to publish IPs authorized to send email on your domain's behalf.*
  
  Removing your origin from this record will result in those emails being classified as spam.

- Example – MX records

  *CBSPs don’t process or forward your emails.*
VULNERABILITY 2: DNS RECORDS

Our findings

- Queried all DNS RR types for every domain
  
  *We extracted and verified each IP address that we found.*

- 28% of domains are vulnerable
  
  - MX records (4,390 domains)
  - TXT records (1,134 domains)
  - Sometimes even A or AAAA records
VULNERABILITY 3: SSL CERTIFICATES

- HTTPS connection between CBSP and origin

  Origin server has to present certificate.
  This certificate contains the domain name.
VULNERABILITY 3: SSL CERTIFICATES

Our findings

- Harvest certificates from all IP addresses
  
  *Data from Project Sonar. ([https://scans.io/study/sonar.ssl](https://scans.io/study/sonar.ssl))
  
  *Censys.io: a new search engine for this data.*

- 9% of domains are revealing their origin by publicly presenting the domain’s certificate
VULNERABILITY 4: IP HISTORY

• “The Internet never forgets”: companies constantly track DNS changes

*Historical databases of previously used IP addresses (e.g. domaintools.com, myip.ms, ...).*

*Your origin IP address might be listed.*

<table>
<thead>
<tr>
<th>No</th>
<th>Website</th>
<th>Old IP Address was</th>
<th>Host was</th>
<th>Date when site was using this IP</th>
<th>Date when it was found that the site had changed IP</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>thome.com</td>
<td>192.230.81.126</td>
<td>192.230.81.126.ip.incapdns.net</td>
<td>03 Feb 2016</td>
<td>16 Feb 2016, 17:17</td>
</tr>
<tr>
<td>3</td>
<td>thome.com</td>
<td>74.63.30.126</td>
<td></td>
<td>11 Nov 2015</td>
<td>15 Dec 2015, 01:29</td>
</tr>
</tbody>
</table>

• Best practice: new IP address after adopting cloud protection
VULNERABILITY 4: IP HISTORY

Our findings

- We queried these IP History databases
  
  We verified each listed historic IP address for all domains.

- 40% of domains have their origin listed in these databases
VULNERABILITY 5: SENSITIVE FILES

- Publicly accessible sensitive files can expose the origin
  Verbose error messages, log files, configuration files, ...

```plaintext
<table>
<thead>
<tr>
<th>SERVER_SIGNATURE</th>
<th>nolvalue</th>
</tr>
</thead>
<tbody>
<tr>
<td>SERVER_SOFTWARE</td>
<td>Apache</td>
</tr>
<tr>
<td>SERVER_NAME</td>
<td>veagsee.org</td>
</tr>
<tr>
<td>SERVER_ADDR</td>
<td>83.137.145.21</td>
</tr>
<tr>
<td>SERVER_PORT</td>
<td>4443</td>
</tr>
<tr>
<td>REMOTE_ADDR</td>
<td>192.168.1.255</td>
</tr>
<tr>
<td>DOCUMENT_ROOT</td>
<td>/domains/veagsee.org/public_html/www/</td>
</tr>
</tbody>
</table>
```
VULNERABILITY 5: SENSITIVE FILES

Our findings

- We searched for files that called `phpinfo()` in 4 fixed locations
  /info.php
  /phpinfo.php
  /test.php
  /phpMyAdmin/phpinfo.php

- 5% of domains have such files and expose their origin in this fashion
VULNERABILITY 6: OUTBOUND CONNECTIONS

- Triggering an origin to connect to you

  *Outbound connections don’t pass through CBSP.*
  *IP address of the origin will be directly visible to destination.*
  *Usually application specific vulnerabilities.*
VULNERABILITY 6: OUTBOUND CONNECTIONS

Our findings

- Triggered a PingBack verification on each web server
  - Web application retrieves the link in the PingBack notification
  - Mostly WordPress installations

- Our own web server tracked incoming connections

- 7% of domains connected to us using their origin IP address
REMAINING VULNERABILITIES

- Temporary exposure
  4% vulnerable

- Origin IP address in Content
  1% vulnerable
ORIGIN-EXPOSING VULNERABILITIES (1)

<table>
<thead>
<tr>
<th>SUBDOMAINS</th>
<th>DNS RECORDS</th>
<th>SENSITIVE FILES</th>
<th>IP HISTORY</th>
</tr>
</thead>
<tbody>
<tr>
<td>In order not to break some protocols, several websites configured subdomains that resolve directly to the origin.</td>
<td>Domains still reveal their web server's IP address through MX, SPF and other DNS records.</td>
<td>Administrators often forget to restrict access to development or log files which expose sensitive information such as the server’s IP address.</td>
<td>A website's IP address can be listed in databases that keep track of historical DNS data.</td>
</tr>
</tbody>
</table>

**Percentages:**
- **SUBDOMAINS:** 43%
- **DNS RECORDS:** 27%
- **SENSITIVE FILES:** 5%
- **IP HISTORY:** 41%
For example, PingBack’s verification mechanism can be leveraged to trigger an outbound connection from your website’s origin, revealing its origin to the recipient.

The domain’s origin IP address can be written in the HTML content of the website.

Administrator temporarily bypassed the cloud protection.

Internet-wide scanners can find the servers that present SSL certificates for the website’s domain name.
“HOW MANY DO YOU HAVE?”

cloudpiercer.org

Thomas Vissers; Tom Van Goethem; Wouter Joosen; Nick Nikiforakis
DEFENSES

How can I prevent my origin IP address from leaking?
PREVENTING ORIGIN EXPOSURE

- Request “fresh” IP address when activating cloud-based security
  *Protects you from historic knowledge attacks*

- Block all non-CBSP requests with your firewall
  *Prevents origin verification and web applications attacks*

- Choose a CBSP that assigns a dedicated IP address to you
  *One-to-one port forwarding solves the non-web protocol limitation*

- Use [cloudpiercer.org](http://cloudpiercer.org) to scan your website
  *Tests all discussed vulnerabilities*
ONLINE TOOL

Discover our online tool to scan for vulnerabilities
CloudPiercer is made available online at https://cloudpiercer.org. We hope that the community will benefit from this service by allowing administrators to discover and eliminate vulnerabilities on their websites, before they are discovered by attackers.
Cloudpiercer Discovery Tool

Researchers have released details of a tool that allows users to discover original Cloudpiercer, which uses a number of techniques to locate origin servers’ IP addresses. The Cloudpiercer tool bundles several previously known methods with some reconnaissance against targets. It’s a reconnaissance tool, not an attack tool. It allows methods to search for a customer’s datacenter IP addresses or netblock(s) to perform an actual DDoS or web application attack.

Cloudpiercer requires verification of ownership of a site for it to be tested. The Cloudpiercer blog has been disabled due to various legal issues.

Cloudpiercer: Is your cloud-protected website really safe?

In October 2015, an academic paper relating to the topic of Cloudpiercer was released. An interesting paper on the topic of the security of cloud-based security solution services was discussed. The cloud-based solution was identified as the weak point in the DDoS mitigation, such as Incapsula.

DDoS mitigation and site vulnerable

DNS rerouting does not eliminate the possibility of bypassing Cloudpiercer. The way to reduce your site’s risk is to use this IP address scanning tool.

Cloudpiercer: Discovery Tool

The researchers have released details of a tool that allows users to discover original Cloudpiercer, which uses a number of techniques to locate origin servers’ IP addresses. The tool bundles several previously known methods with some reconnaissance against targets. It’s a reconnaissance tool, not an attack tool. It allows methods to search for a customer’s datacenter IP addresses or netblock(s) to perform an actual DDoS or web application attack.

Cloudpiercer requires verification of ownership of a site for it to be tested. The Cloudpiercer blog has been disabled due to various legal issues.

Cloudpiercer: Is your cloud-protected website really safe?

In October 2015, an academic paper relating to the topic of Cloudpiercer was released. An interesting paper on the topic of the security of cloud-based security solution services was discussed. The cloud-based solution was identified as the weak point in the DDoS mitigation, such as Incapsula.

DDoS mitigation and site vulnerable

DNS rerouting does not eliminate the possibility of bypassing Cloudpiercer. The way to reduce your site’s risk is to use this IP address scanning tool.
cloudpiercer.org

Thomas Vissers, Tom Van Goethem, Wouter Joosen, Nick Nikiforakis