

[Register](#)  
[Login to your account](#)  
Welcome Guest  
[Advertise](#)  
[About Us](#)

# SECTIONS ▼



- [Authors](#)
- [Slideshows](#)
- [Video](#)
- [Reports](#)
- [White Papers](#)
- [Events](#)
- [Black Hat](#)
- [Attacks/Breaches](#)
- [App Sec](#)
- [Cloud](#)
- [Endpoint](#)
- [Mobile](#)
- [Perimeter](#)
- [Risk](#)
- [Operations](#)
- [Analytics](#)
- [Vulns/Threats](#)



- [Login to your account](#)
- [Register](#)
- [Login to your account](#)
- [Register](#)
- [About Us](#)
- [Advertise](#)

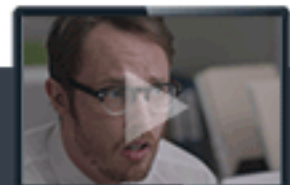


Search Dark Reading

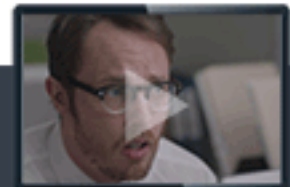


- [Facebook](#)
- [Twitter](#)
- [LinkedIn](#)
- [Google+](#)
- [RSS](#)





**Watch the Video**



[Watch the Video](#)



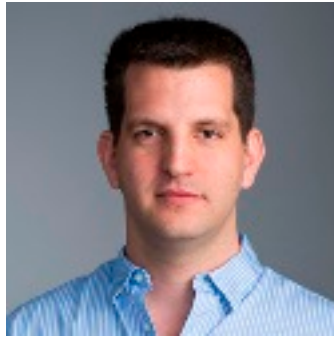
Join us live at



Search Dark Reading



Endpoint



Amir Shaked  
Commentary

Connect Directly



 1 Comment

[Comment  
Now](#)

[Login](#)

   
100%0%

 Like 86  Tweet  Share  218  G+1  15

## Brute-Force Botnet Attacks Now Elude Volumetric Detection

**It just became harder to distinguish bot behavior from human behavior.**

*Inbar Raz, Principal Researcher, PerimeterX, also contributed to this commentary.*

Ask just about anyone the question “What distinguishes an automated (bot) session from a human-driven session?” and you'll almost always get the same first answer: “Speed.” And no wonder - it's our first intuition. Computers are just faster.

If you focus the question on credential brute-forcing, then it's even more intuitive. After all, the whole purpose of a brute-force attack is to cover as many options as possible, in the shortest possible time. Working quickly is just elementary, right?

Well, it turns out that this is not always the case. Most defenders, if not all, are already looking at speed and have created volumetric detections that are nothing more than time-based signatures. And that works, most of the time. But the attackers are getting smarter every day, and changing their attack methods. Suddenly, checking speed is no longer enough.

On the first week of October, we detected a credentials brute-force attack on one of our customers that commenced around 03:30am UTC. The attack, which lasted a few minutes shy of 34 hours, spanned a whopping 366,000 login attempts. Sounds like an easy case - 366K over 34 hours is over 10,000 attempts per hour.

But an easy catch? Not by existing volumetric detections, because the attack did not originate from one single IP address. In fact, we discovered that well over 1,000 different IP addresses participated in this attack. Let's look at the distribution of attempts:

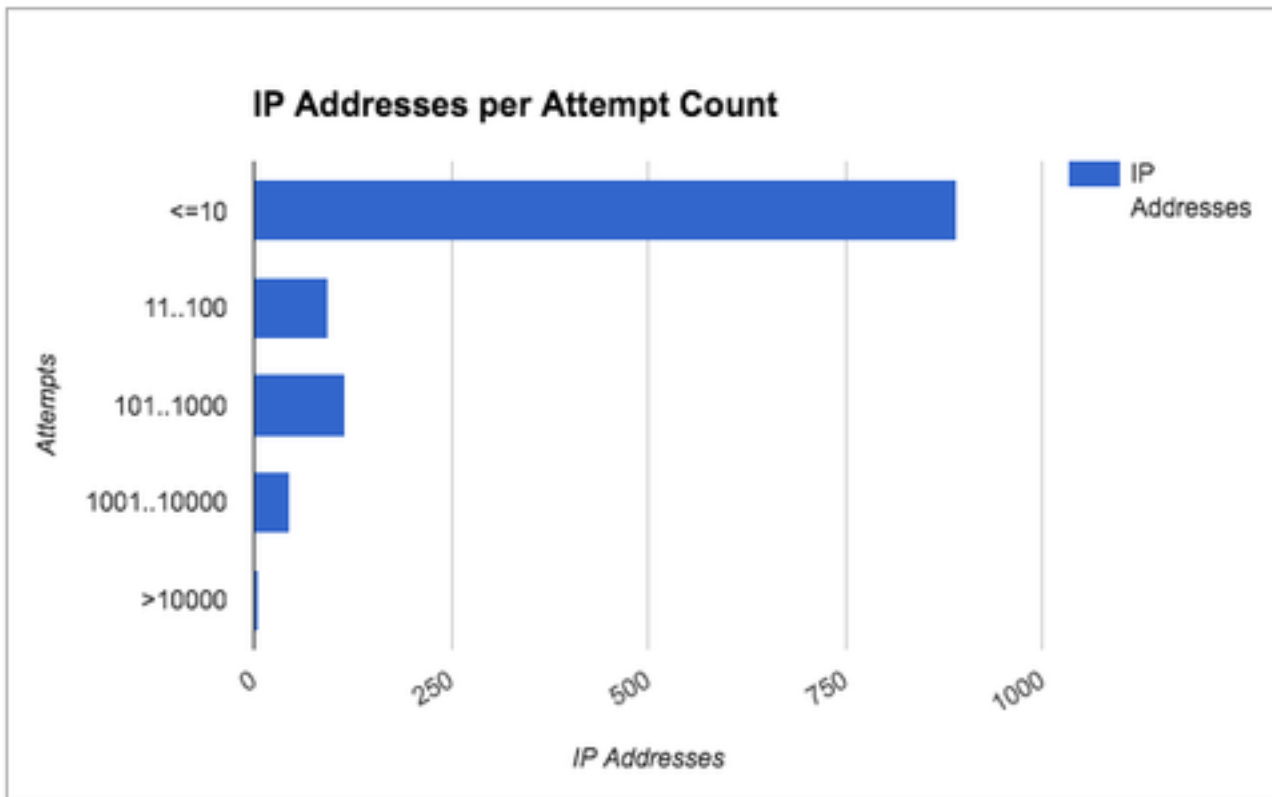


Image Source: PerimeterX

Of all the participating IP addresses, the vast majority (over 77%) of them appeared up to 10 times only, during the entire attack. While the minority may trigger a volumetric detection, 77% percent of the attacking IP addresses would go unnoticed.

One can argue that counting failed login attempts would come in handy here. And it indeed could, except that many of the brute-force attacks don't actually enumerate on passwords tirelessly. Instead, they try username/password pairs that were likely obtained from leaked account databases, gathered from other vulnerable and hacked sites. Since many people use the same password in more than one place, there is a good chance that some, if not many, of the login attempts will actually be successful.



Sponsored Content

### Don't Let Security Put the Brakes on DevOps

The rise of agile software development and DevOps methods have brought speed and quality benefits, but they have inadvertently put a huge strain on security organizations.

Sponsored By CloudPassage

### How Motivated Attackers Adapt

On a different attack we observed, nearly 230,000 attempts at logging in over 20 minutes were performed from over 40,000 participating IP addresses. The vast majority of IP addresses were the origin point of 10 or fewer attempts. A volumetric detection would simply miss this attack.

In comparison, a common volumetric detector is usually set to between 5 and 30 as a minimum, depending on the site's specific behavior. Our data suggest that motivated attackers will adapt and adjust their numbers to your threshold, no matter how low it is. We also observed that the attack was incredibly concentrated within a very short detection window of only about 20 or 25 seconds.

### Fake User Creation Attack

Let's look at one last distributed attack, on yet another client. This time, the attack is not about credentials brute-forcing but rather fake user creation. In this example, the largest groups of IP addresses used per attempt count were those that committed only 1 or 2 attempts:

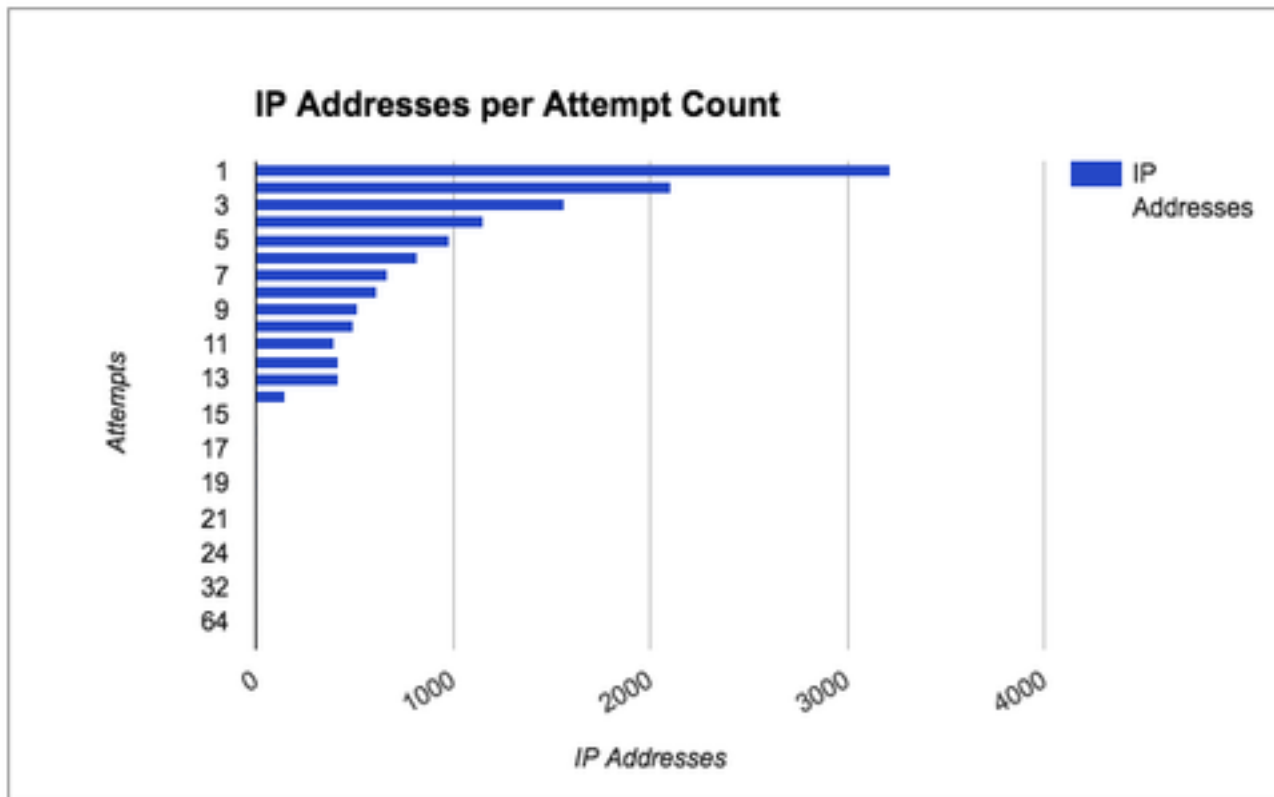


Image Source: PerimeterX

The entire attack was conducted in less than six hours.

How do the attackers get so many IP addresses to attack from? The answer lies in analyzing the IP addresses themselves. Our research shows that 1% were proxies, anonymizers or cloud vendors, and the other 99% were private IP addresses of home networks, likely indicating that the attacks were performed by some botnet (or botnets) of hacked computers and connected devices. Furthermore, the residential IP addresses constantly change (as in any home) rendering IP blacklisting irrelevant, and even harmful for the real users' experience.

### Suspicious Indicators

We included in this post just a few representative examples (out of many more we detected) of large-scale attacks originating from thousands of IP addresses over a short time span. In the majority of these cases, detection was achieved by examining how users interacted with the website. The suspicious indicators included users accessing only the login page, filling in the username and password too fast or not using the mouse.

The implication of these attacks vary. They include theft of user credentials as well as fake user account creation, which in turn leads to user fraud, spam, malware distribution and even layer-7 DDoS on the underlying web application.

In conclusion, volumetric detections are *simple* and *useful*, but they are not *sufficient*. The attackers continue to improve their techniques, bypassing old-fashioned defenses. The new frontier in defense is in distinguishing bot behavior from human behavior – and blocking the bots.

### Related Content:

- [Hacker 2016 To-Do List: Botnet All The Things!](#)
- [From Carna To Mirai: Recovering From A Lost Opportunity](#)
- [IoT DDoS Attack Code Released](#)

*Inbar Raz has been teaching and lecturing about Internet security and reverse engineering for nearly as long as he's been doing that himself: He started programming at the age of 9 and reverse engineering at the age of 14. Inbar specializes in outside-the-box approaches to analyzing security and finding vulnerabilities; the only reason he's not in jail right now is because he chose the right side of the law at an earlier age. These days, Inbar is the principal researcher at PerimeterX, researching and educating the public on automated attacks on websites.*

*Amir Shaked is a software engineer and security researcher. He entered the software world at the age of 14 and has been developing and researching ever since at various startups and companies. In recent years he managed several groups and recently started leading the research ... [View Full Bio](#)*

### More Insights

#### Webcasts

[Cybersecurity] Costs, Risks, & Benefits

[Analytics] Make the Most of Your Data's Potential in 2017

#### More Webcasts

#### White Papers

Speed Up Incident Response & Discover Critical Attack Details

[Case Study] Xero chooses CloudPassage Halo for Workload Security at DevOps Speed

#### More White Papers

#### Reports

Ransomware Report

How Enterprises Are Attacking the IT Security Enterprise

#### More Reports

### Comments

[Newest First](#) | [Oldest First](#) | [Threaded View](#)



[Simonjonzie,](#)

User Rank: Apprentice

12/26/2016 | 11:33:38 AM

[Login](#)



50%50%

#### Good article

This is very true. Most bots these days fly right under the radar. You can't block based on IP because it's a constant game of whack a mole. Hackers that know what they're doing will constantly change IPs using cloud providers to spin up different IP blocks. It takes a very sophisticated system to identify bots. They will send a couple requests from a thousand IPs at once, instead of thousands of requests from a single IP. Rate limiting cannot detect this and it looks very human in nature. There is a great article that talks about this at botnetremoval dot com. It even suggests what to consider in your entire security stack, saying that you need bot mitigation as an entirely separate solution.

[Reply](#) | [Post Message](#) | [Messages List](#) | [Start a Board](#)

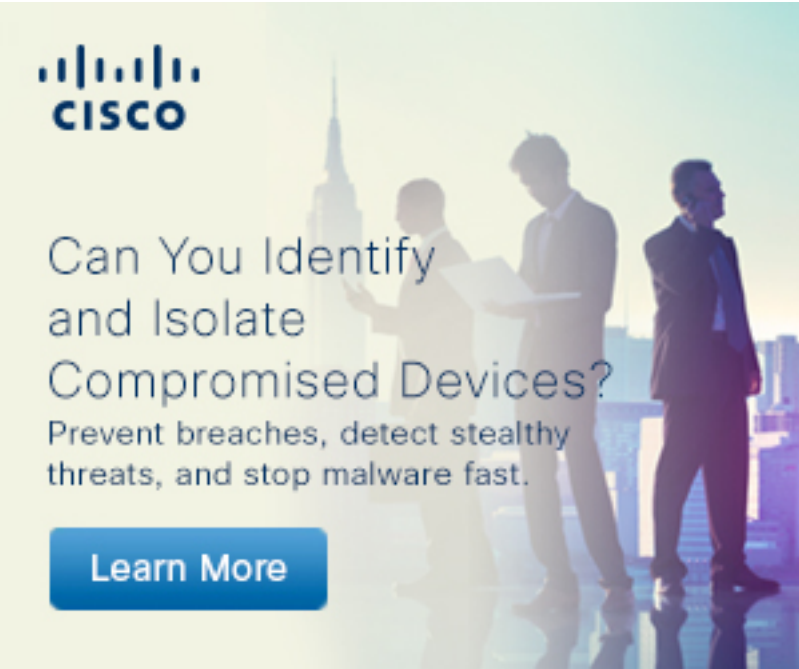





# Can You Identify and Isolate Compromised Devices?

Prevent breaches, detect stealthy threats, and stop malware fast.

[Learn More](#)



# Can You Identify and Isolate Compromised Devices?

Prevent breaches, detect stealthy threats, and stop malware fast.

[Learn More](#)



[Subscribe to Newsletters](#)

- Live Events

Webinars



More UBM Tech  
Live Events

**Interop ITX - The Independent Conference for Tech Leaders**

**Attend the Leading Unified Comms & Collaboration Event**

**Systems Management & Network Design Track at EC17**

White Papers

■ [Speed Up Incident Response & Discover Critical Attack Details](#)

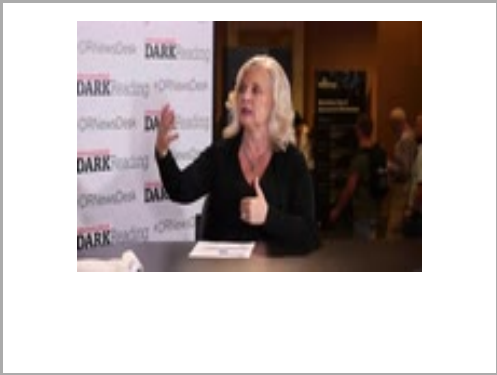
■ [\[IoT\] 4 Ways Predictive Maintenance Streamlines Manufacturing](#)

- [Gartner Research: Use SIEM for Targeted Attack Detection](#)
- [\[Data Center\] 5 Benefits of Having USB Ports on Your Rack PDUs](#)
- [\[Cybersecurity\] 5 Things Every Business Executive Should Know](#)

More White Papers



Video



All Videos

Cartoon







## Backing Up the Internet of Things

[Post a Comment](#)

[Cartoon Archive](#)

Current Issue



### Five Things Every Business Executive Should Know About Cybersecurity

Don't get lost in security's technical minutiae - a clearer picture of what's at stake can help align business imperatives with technology execution.

[Download This Issue!](#)

[Back Issues | Must Reads](#)

[Flash Poll](#)

**What's missing from your incident response plan? (Pick all that apply.)**

- ☐ Access to activity logs
- ☐ An up-to-date network diagram
- ☐ Blueprint for public disclosure

- ☐ Hostname-IP address maps
- ☐ IR fire drills before the event
- ☐ Plan for finding malicious files after the breach
- ☐ We don't have an incident response plan
- ☐ Other (Please explain in the comments)

Submit

All Polls

Reports

InformationWeek  
**DARK**Reading  
reports

reports.informationweek.com

December 2016

# Secure Application Development: New Best Practices

The transition from DevOps to SecDevOps is combining with the move toward cloud computing to create new challenges – and new opportunities – for the information security team.

Sponsored by CloudPassage



## Secure Application Development - New Best Practices

The transition from DevOps to SecDevOps is combining with the move toward cloud computing to create new challenges - and new opportunities - for the information security team. Download this report, to learn about the new best practices for secure application development.

Download Now!

- Dark Reading Strategic Security Report: The Impact of Enterprise Data Breaches 0 comments
- The Top Cybersecurity Risks And How Enterprises Are Responding 0 comments





10 Cocktail Party Security Tips From The Experts

1 comments | Read | Post a Comment

What To Watch For With Ransomware: 2017 Edition

2

7 Ways To Fine-Tune Your Threat Intelligence Model

3

More Slideshows

Twitter Feed



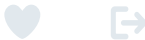
**divinereikitraining** @juliefenn2012



The 7 Best Social Engineering Attacks Ever [darkreading.com/the-7-best-soc...](#) via @DarkReading



**The 7 Best Social Engineering Attacks Ever**  
Seven reminders of why technology alone isn't enough to keep you secure.  
[darkreading.com](#)



2m



**Ercument B.Sumnulu** @ErcumentSumnulu



Ransomware: How A Security Inconvenience Became The Industry's Most-Feared Vulnerability  
[darkreading.com/endpoint/ranso...](#) via @DarkReading



**Ransomware: How A Security Inconvenience Became The Industry's Most-Feared Vulnerability**  
There are all sorts of ways to curb ransomware, so why has it spread so successfully?  
[darkreading.com](#)



4m



## Enterprise Vulnerabilities From DHS/US-CERT's National Vulnerability Database

### [CVE-2013-7445](#)

Published: 2015-10-15

The Direct Rendering Manager (DRM) subsystem in the Linux kernel through 4.x mishandles requests for Graphics Execution Manager (GEM) objects, which allows context-dependent attackers to cause a denial of service (memory consumption) via an application that processes graphics data, as demonstrated b...

### [CVE-2015-4948](#)

Published: 2015-10-15

netstat in IBM AIX 5.3, 6.1, and 7.1 and VIOS 2.2.x, when a fibre channel adapter is used, allows local users to gain privileges via unspecified vectors.

### [CVE-2015-5660](#)

Published: 2015-10-15

Cross-site request forgery (CSRF) vulnerability in eXtplorer before 2.1.8 allows remote attackers to hijack the authentication of arbitrary users for requests that execute PHP code.

### [CVE-2015-6003](#)

Published: 2015-10-15

Directory traversal vulnerability in QNAP QTS before 4.1.4 build 0910 and 4.2.x before 4.2.0 RC2 build 0910, when AFP is enabled, allows remote attackers to read or write to arbitrary files by leveraging access to an OS X (1) user or (2) guest account.

### [CVE-2015-6333](#)

Published: 2015-10-15

Cisco Application Policy Infrastructure Controller (APIC) 1.1j allows local users to gain privileges via vectors involving addition of an SSH key, aka Bug ID CSCuw46076.

---

## Dark Reading Radio

### Archived Dark Reading Radio

#### **The Coolest Hacks of 2016**

In past years, security researchers have discovered ways to hack cars, medical devices, automated teller machines, and many other targets. Dark Reading Executive Editor Kelly Jackson Higgins hosts researcher Samy Kamkar and Levi Gundert, vice president of threat intelligence at Recorded Future, to discuss some of 2016's most unusual and creative hacks by white hats, and what these new vulnerabilities might mean for the coming year.

[FULL SCHEDULE](#) | [ARCHIVED SHOWS](#)

[About Us](#)

[Twitter](#)

[Contact Us](#)

[Facebook](#)

[Customer Support](#)

[LinkedIn](#)

[Sitemap](#) &nbsp; [Reprints](#)

[Google+](#)

[RSS](#)



Technology Group

Black Hat	Enterprise Connect	HDI	Network Computing
Content Marketing Institute	Fusion	ICMI	No Jitter
Content Marketing World	GDC	InformationWeek	VRDC
Dark Reading	Gamasutra	Interop ITX	

[Terms of Service](#) | [Privacy Statement](#)

COMMUNITIES SERVED

- Content Marketing
- Enterprise IT
- Enterprise Communications
- Game Development
- Information Security
- IT Services & Support

WORKING WITH US

- Advertising Contacts
- Event Calendar
- Tech Marketing
- Solutions
- Contact Us
- Licensing

Copyright © 2017 UBM, All rights reserved