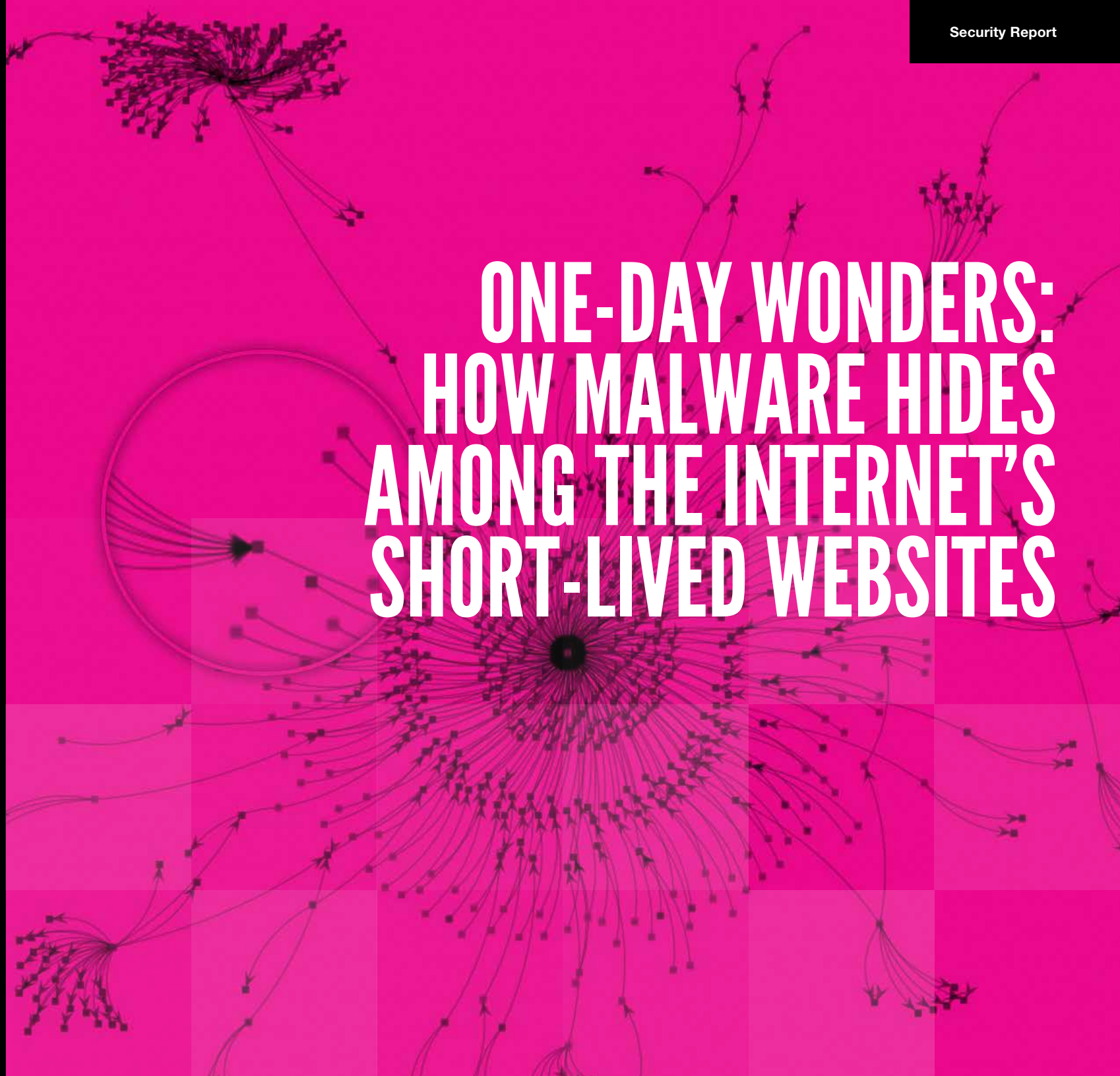
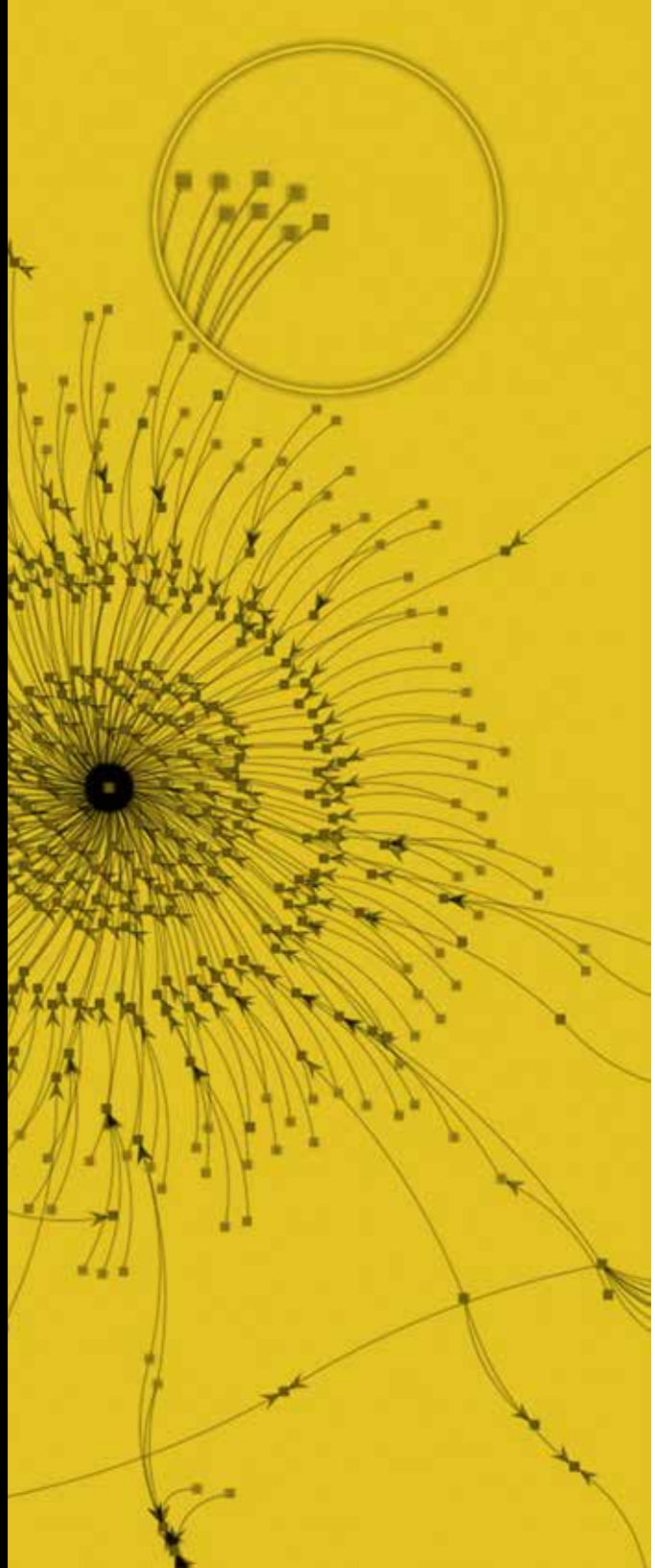
BLUE COAT®

Security Empowers Business



ONE-DAY WONDERS: HOW MALWARE HIDES AMONG THE INTERNET'S SHORT-LIVED WEBSITES



Executive Summary

Anyone can quickly build and launch a website, and that fact has contributed to the prolific spread of the Internet. But how long do newly built websites last, and what are the security implications of “One-Day Wonders,” websites that exist for less than 24 hours?

For the first time, the Blue Coat Security Labs team has looked into the nature of the hostnames that make up the web to determine how ephemeral they really are. To understand more about these One-Day Wonders, their purpose, function and links to other activities, the Blue Coat research team looked at geographical and domain level data sets.

During the investigation, the Blue Coat research team analyzed more than 660 million unique hostnames – not simply unique URLs but unique sub-domains and other sub-sites – from a 90-day period, or one hostname for every 10.6 people in the world, and found that fully 71 percent, or 470 million, of all hostnames analyzed during a 90-day period only appeared for a single 24-hour period (see Figure 1).

Each day there is a new One-Day Wonder for every 15 people on the planet. Simply put – there are a lot of new, unknown, transient sites being used every day.

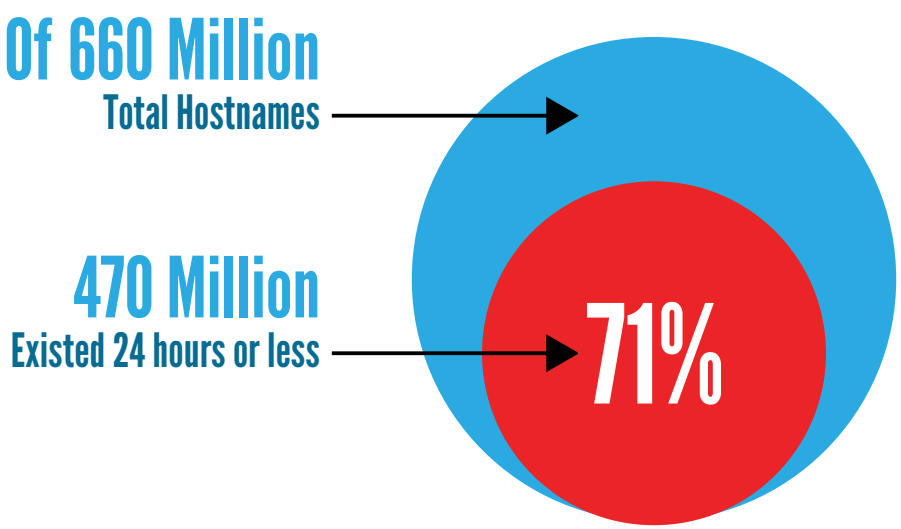


Figure 1: How Long Do Unique Hostnames Exist?
Source: Blue Coat Security Labs, 90-day period of total hostnames.

Sites considered One-Day Wonders are essential to legitimate Internet practices and don't necessarily pose security concerns. The majority of the One-Day Wonders were associated with Content Delivery Networks or blogging platforms. In one case, one of the top ten most prolific creators of One-Day Wonders was the most popular pornography site on the Internet.

While the majority of these One-Day Wonders were not malicious, the sheer volume of them provides ideal cover for malicious activity, including bot communications with command and control servers. Of the top 50 parent domains that most frequently used One-Day Wonders, 22 percent were malicious. These domains use short-lived sites to facilitate attacks and manage botnets, taking advantage of the site being "new and unknown" to evade security solutions.

For organizations fighting ongoing battles against cyber attacks, two key lessons can be drawn from this research:

- Security controls must be informed by automated, real-time intelligence that can identify and assign risk levels to these One-Day Wonders. Static or slow-moving defenses do not suffice to protect users and corporate data.
- Policy-based security controls must be able to act on real-time intelligence to block malicious attacks.

In short, understanding what One-Day Wonders are and how they are used is the key to building a better security posture.

Terminology

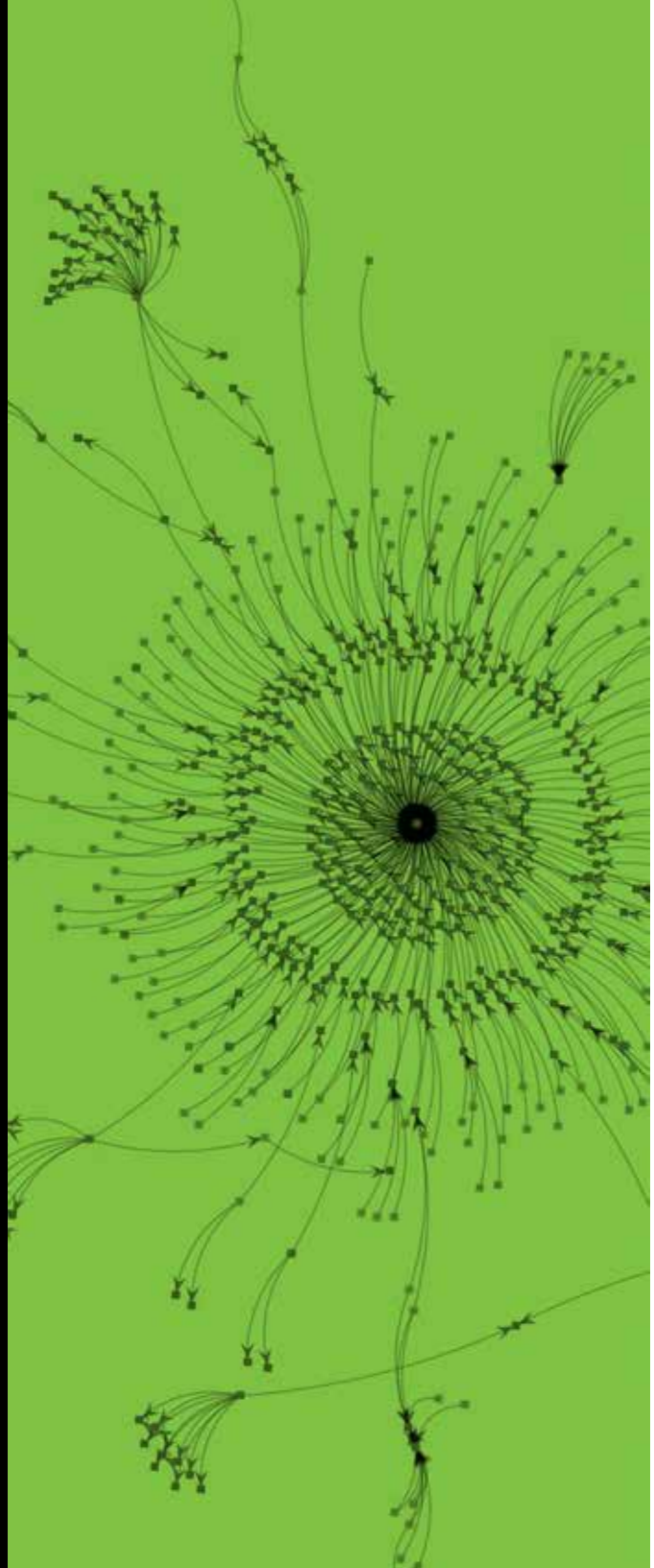
There are several terms related to hostnames, domains, URLs and IP addresses used in this research. Many of our readers already have a strong background with this terminology, but for those who don't, here is a short, very high-level refresh.

Let's use Wikipedia as an example:

Domain name: wikipedia.org
Hostnames: en.wikipedia.org (one hostname per language or nearly 300)
Unique URLs: http://en.wikipedia.org/wiki/Milli_Vanilli (one per entry under each hostname or tens of millions)

These addresses can either be textual (en.wikipedia.org) or numerical IP addresses 1.2.3.4.

For more detailed information on these terms please visit www.wikipedia.org.



One-Day Wonders Power the Internet

Over a 90-day analysis window Blue Coat conducted a detailed investigation into more than 660 million unique hostnames requested by 75 million global users. While this number is significant as the starting point for the raw analysis, more notable was the number of sites that persisted for less than 24 hours across the 90-day window. These One-Day Wonders, as they quickly became known, become accessible and go offline within a day.

Over the course of just three months, 71 percent, about 470 million hostnames, were One-Day Wonders. Even given the dynamic nature of the Internet and how quickly new services are switched on and off, this percentage seemed high.

Most One-Day Wonders are legitimate and exist to deliver a better user experience. Thus, it is not surprising where we see the bulk of activity related to these One-Day Wonders. The primary Top Level Domain (TLD) where activity takes place is .com. As the most prolific TLD, .com represents nearly three-quarters of all One-Day Wonders, as illustrated in Figure 2. In fact, it is 2.5 times higher than the aggregate of all other TLDs. Clearly, One-Day Wonders exist in plain sight – not utilizing more exotic TLDs to obfuscate their behavior.

Rank	TLD	Domains (%)
1	.com	**71.88**
2	.net	**18.14**
3	.info	**1.81**
4	.de	**0.77**
5	.org	**0.76**
6	.uk	**0.45**
7	.br	**0.44**
8	.ru	**0.39**
9	.fr	**0.34**
10	.nl	**0.28**

Figure 2: Top 10 Top Level Domain (TLD) Rankings

Source: Blue Coat Security Labs, 90-day period of total hostnames.

For example, a review of data showing which geographies are responsible for the On-Day Wonders shows that the United States (US) and China (CN), as illustrated in **Figure 3**, represent a combined total of almost 40 percent, which is similar to the percent of IPv4 IP addresses they own.

Given that the U.S. and China have the largest IPv4 address allocations (the U.S. has 36 percent and China has 7.5 percent), the activity across their large address space naturally ranks them highest.

For countries such as Brazil that were allotted just 236 IP addresses per 1,000 people, compared to 4,911 per 1,000 people in the U.S., One-Day Wonders deliver greater leverage from the addresses they do own. It's not surprising, then, that Brazil is responsible for creating 3.8% of all One-Day Wonders when it has just 1.1 percent of all IPv4 IP addresses.

These results demonstrate how the inequity among IPv4 address distribution can be alleviated with One-Day Wonders. They also add further evidence that One-Day Wonders are largely legitimate and exist in plain sight.

Rank by Assigned IPv4 Addresses (%)		Rank by URLs Generated (%)	
United States	**35.9**	**28.8**	United States
China	**7.7**	**11.1**	China
Japan	**4.7**	**4.6**	Japan
United Kingdom	**2.9**	**4.2**	United Kingdom
Germany	**2.8**	**3.8**	Brazil
South Korea	**2.6**	**3.3**	France
France	**2.2**	**3.2**	South Korea
Canada	**1.9**	**3.0**	Germany
Italy	**1.2**	**2.8**	Russia
Brazil	**1.1**	**2.2**	Italy

Figure 3: Where are One-Day Wonders Used? Ranking by Country.

Source: Google's Fusion Tables.

One-Day Wonders Power Popular Internet Services

A deeper dive into parent domains sheds light on how these One-Day Wonders are used to facilitate day-to-day Internet activities. Figure 4 lists the 10 most frequent generators of One-Day Wonders.

Rank	Parent Domain	Domains (%)	Description
1	*.gstatic.com	**46.45**	Associated with Google
2	*.cedexis-radar.net	**5.53**	Web performance optimization company
3	*.cloudfront.net	**4.61**	Associated with Amazon.com
4	*.llnwd.net	**4.41**	Web acceleration for LimeLight Networks
5	*.yahoodns.net	**1.27**	DNS services for Yahoo
6	*.blogspot.com	**1.06**	Free webhosting service for blogs
7	*.xvideos.com	**0.84**	Free pornographic video sharing
8	*.tumblr.com	**0.67**	Micro blogging platform and social networking website
9	*.wordpress.com	**0.50**	Free webhosting service for blogs
10	*.rncdn3.com	**0.49**	Internet hosting company Reflected Networks

Figure 4: Top 10 Parent Domains Using One-Day Wonders

Source: Blue Coat Security Labs, 90-day period of total hostnames.

A number of the top 10 creators of One-Day Wonders are organizations such as Google, Amazon and Yahoo that have a substantial Internet presence, as well as web optimization companies that help accelerate the delivery of content. The shared trait among these types of organizations is the use of Content Delivery Networks (CDNs).

The speed and reliability CDNs provide are essential to their operation. It appears these organizations use unique subdomains (and sub-sub-domains) to keep track of content in the CDN. This could be to identify a particular user, session, or request, and once that user/session/request is finished, the sub-sub-domain isn't used again. A byproduct of these CDN architectures is the proliferation of One-Day Wonders.

An analysis of Internet behavior wouldn't be complete without contemplating the role pornography plays. According to Wikipedia, XVideos, a free pornographic video sharing site, is the 40th most popular site on the Internet and is considered the most popular pornographic website in the world. It generates enough One-Day Wonders to rank seventh on the list.

Blogging sites such as BlogSpot, Tumblr and WordPress host tens of millions of individual blogs at the subdomain level. While very few of these get consistent traffic, making them appear to be One-Day Wonders, there are also a number of malicious and shady sub-sites on these platforms as well.

Malicious One-Day Wonders Hiding in Plain Sight

We wouldn't be writing this report if there weren't a darker side to the One-Day Wonders.

Blue Coat security researchers have long observed that malnet operators love to generate large numbers of subdomains on a smaller set of evil domains. These transient sites are a critical component of mass attack support infrastructures. They both ensure additional bots can easily be added to an existing army and give cyber criminals the ability to manage their botnets for a longer period of time, increasing the return on investment for any given attack.

For example, One-Day Wonders can be used to build dynamic command and control architectures that are scalable, difficult to track and easy to implement. Alternatively, they can be used to create a unique subdomain for each spam email to throw off spam or web filters.

One-Day Wonders are particularly popular with cyber criminals because they:

- **Keep security solutions guessing**: Dynamic domains are harder to thwart than static domains
- **Overwhelm security solutions**: Generating a high volume of domains increases the chances that some percentage will be missed by security controls
- **Hide from security solutions**: By simply combining One-Day Wonders with encryption and running incoming malware and/or outgoing data theft over SSL, organizations are typically blind to the attack, impacting their ability to prevent, detect and respond

Looking back through the top 50 – just two spots removed from the top 10 parent domains at number 12 – is a malicious site (see Figure 5).

Rank	Parent Domain	Domains (%)	Description
12	*.1-tr-18su-ka-8dow-56-oo9-13swx-r-k-ife-0nj-rnq-ihb-dd-p-1-0-z-a.info	**0.43%**	Trojan dialer

Figure 5: Top Malicious Domain

Source: Blue Coat Security Labs, 90-day period of total hostnames.

This .info domain is actually a command and control server for a Trojan dialer. Over the 90-day analysis window it had more than 1.3 million subdomains.

And this wasn't the only one. Across the top 50 parent domains, there are 10 more similar parent domains that were identified as being part of command and control infrastructures. Thus 22 percent of the top 50 parent domains analyzed are used for malicious activities. Further research into this family of malicious domains revealed that they are also extremely active.

Figure 6: Prevalence of Malicious Domains

Source: Blue Coat Security Labs, 90-day period of total hostnames.

Mitigating Threats Associated with One-Day Wonders

With such a vast ecosystem of hostnames being turned on and off every day, this discovery should convince any organization that static security controls predicated on fixed lists of known, bad elements cannot provide sufficient protection.

The rapid building up and tearing down of new and unknown sites destabilizes many existing security controls, reinforcing the need for global, real-time threat intelligence that can accurately discover, assess and distribute intelligence in an automated way.

Being able to sift through One-Day Wonders to separate the noise from the threats is critical to maintaining a strong security posture. Key requirements and considerations include:

- **Real-time intelligence**: Organizations should utilize security controls that have real-time intelligence to identify One-Day Wonders and block access to those that are malicious. A simple black list of known malicious sites will not address the issue as One-Day Wonders are specifically engineered to thwart such static approaches.
- **Threat risk levels**: Having solutions in place that can comprehensively assess and assign a risk value based on a number of factors is crucial for setting policies that can help automate defenses and prioritizing incidents. Security solutions need to understand context around domains and IP addresses, including site popularity, links to other sites, number of other sites hosted on the same IP address and the ratings of those sites. Simple intelligence based on URLs and IP addresses provides little value anymore.
- **Baseline of hostnames**: Pattern discovery can help create a baseline of transient hostnames. Once this baseline is discovered, the detection of an anomaly from that baseline may constitute a potential compromise leading to alerts and other threat mitigation actions.
- **Granular policy controls**: Security controls need to allow for detailed policy creation based on the real-time intelligence, threat risk levels and hostname baselines to help automate defenses and fortify security postures.

Attribution

A special thanks to all the Blue Coat security researchers who helped generate this report, including Tim van der Horst, Chris Larsen and Patrik Runald.

v.BC-ONE-DAY-WONDERS-EN-v1e-0814

BLUE COAT®

Security Empowers Business

Blue Coat Systems Inc.
www.bluecoat.com

Corporate Headquarters
Sunnyvale, CA
+1.408.220.2200

EMEA Headquarters
Hampshire, UK
+44.1252.554600

APAC Headquarters
Singapore
+65.6826.7000