

Hot SUMMER Bytes



Following a busy and successful quarter, Cyber Security welcomes you to the Cyber Security News-letter: Summer Edition! Encompassing June, July, and August months, We packed this publication full of the hottest summer security news, aggregated team metrics and of course, a new crypto-challenge. Cyber Security personally thanks you for your patience and loyal readership. Regular monthly publications resume starting September 2017.

[AlphaBay](#) | [Girl Scouts](#) | [Stats](#) | [DMV](#) | [Digital Defenses](#) | [Dark Web](#) | [Writers Block](#) | [Crypto Challenge 3.0](#)

AlphaBay the Largest **Shut** Online Dark Market **Down**

The Justice Department seized the largest criminal marketplace on the Internet, AlphaBay, which operated for over two years on the dark web and was used to sell deadly illegal drugs, stolen and fraudulent identification documents and access devices, counterfeit goods, malware and

other computer hacking tools, firearms, and toxic chemicals throughout the world. The international operation to seize AlphaBay's infrastructure was led by the United States and involved cooperation and efforts by law enforcement authorities

This is likely one of the most important criminal investigations of the year...

-Attorney General J. Sessions

in Thailand, the Netherlands, Lithuania, Canada, the United Kingdom, and France, as well as the European law enforcement agency Europol.

“This is likely one of the most important criminal investigations of the year – taking down the largest dark net marketplace in history,” said Attorney General Jeff Sessions.”

Read the full press release: [here](#).

Learn more about the “Dark Web” on page 5: [here](#).



paloalto
NETWORKS



girl scouts

Palo Alto Networks, and Girl Scouts of the USA (GSUSA) announced that they will join forces to deliver the first-ever national Girl Scout Cybersecurity badges for girls in grades K–12. Girl Scout badges are insignia Girl Scouts earn and display on their uniforms to demonstrate their mastery of a given topic. Led by a panel of expert cybersecurity advisers, GSUSA and Palo Alto Networks expect to roll out the first in a series of 18 Cybersecurity badges to Girl Scouts throughout the United States in September 2018.

According to the latest Cybersecurity Jobs Report by Cybersecurity Ventures, the worldwide deficit of qualified cybersecurity professionals will reach 3.5 million by 2021. A deficit of this magnitude can inhibit the industry's ability to prevent cyber breaches, and the challenge is compounded by the growing frequency and sophistication of cyber-attacks. Getting ahead of tomorrow's threats requires a larger, diverse and innovative team of problem solvers.

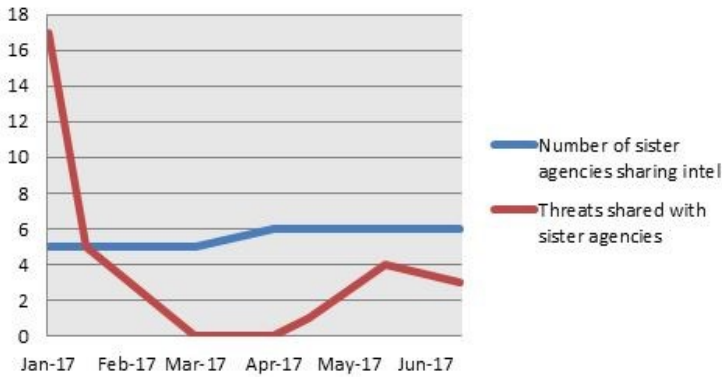
Read the article [here](#).

About Girl Scouts of the USA

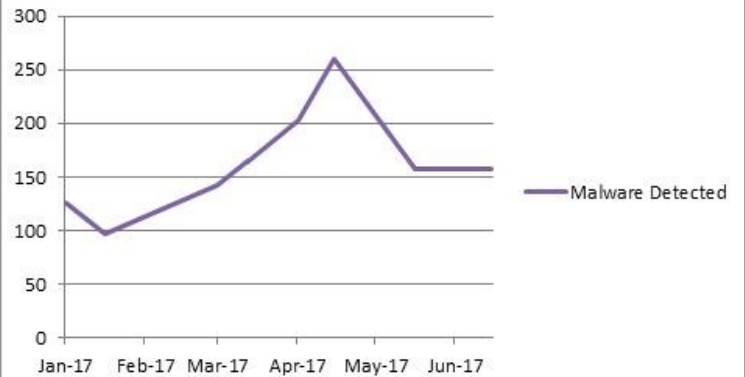
We're 2.6 million strong—1.8 million girls and 800,000 adults who believe in the power of every G.I.R.L. (Go-getter, Innovator, Risk-taker, Leader) to change the world. Our extraordinary journey began more than 100 years ago with the original G.I.R.L., Juliette Gordon "Daisy" Low. On March 12, 1912, in Savannah, Georgia, she organized the very first Girl Scout troop, and every year since, we've honored her vision and legacy, building girls of courage, confidence, and character who make the world a better place. We're the preeminent leadership development organization for girls. And with programs from coast to coast and across the globe, Girl Scouts offers every girl a chance to practice a lifetime of leadership, adventure, and success. To volunteer, reconnect, donate, or join, visit www.girlscouts.org.

< Cyber Stats />

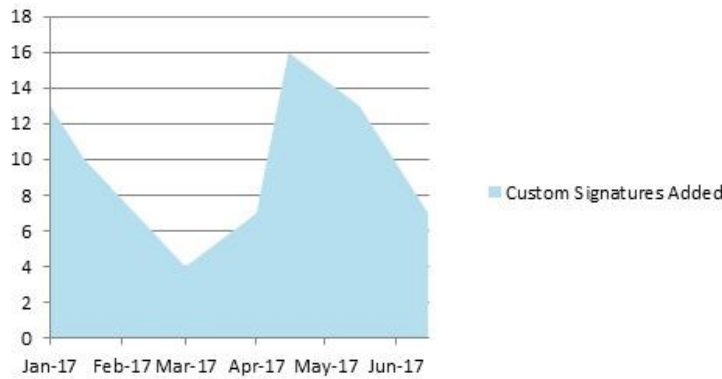
Threat Intelligence



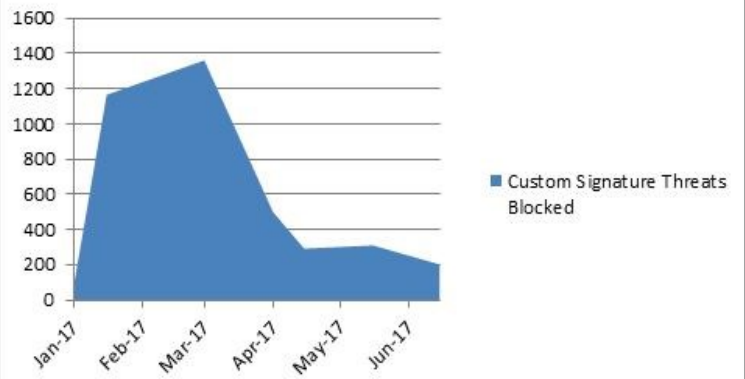
Endpoint Security



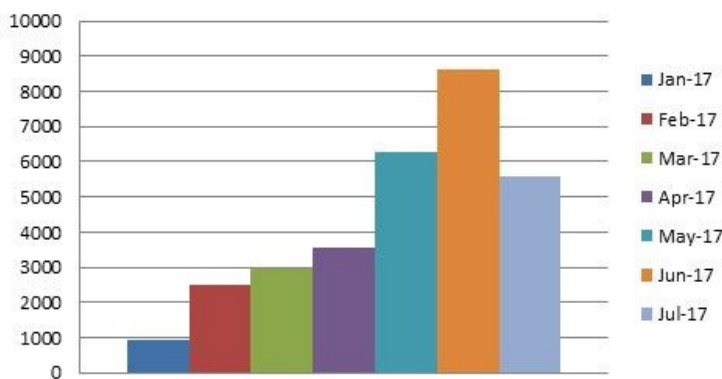
Intrusion Prevention



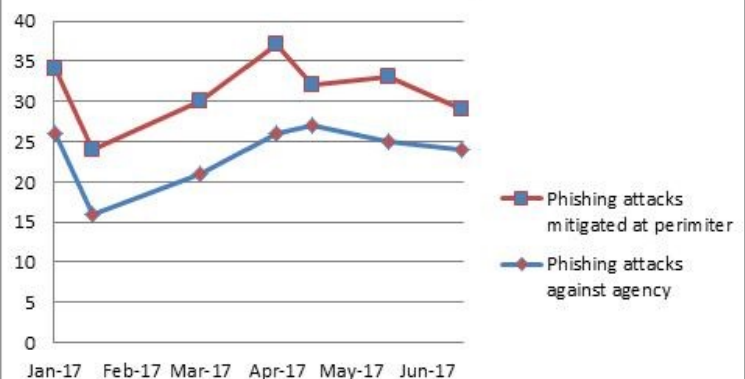
Intrusion Prevention



Threats Blocked



Email Security



DMV Warns Consumers of Fake Ticket Email Hoax

[The New York State Department of Motor Vehicles \(DMV\)](#) is cautioning consumers against an email "phishing" campaign that sends a notice to email users stating they must pay a ticket within 48 hours or their license will be revoked. While the notice is made to appear as if it comes from DMV, it is a hoax.

The fake emails pretend to be from DMV, and report that the State Police has advised DMV that the recipient has several outstanding traffic violations. It then provides two links to either plead guilty or to refute the tickets. The links direct unsuspecting users to a malicious download that may expose your computer to a virus. If you receive one of these emails, delete the email immediately. Do not click on any links in the email and do not forward the email.

Read the full press release [here](#).



Building a Digital Defense with an Email Fortress

Phishing schemes are often just the start -- leading to potential ransomware attacks, business-e-mail-compromise scams, and more. From the lowest level employee up to the CEO, your e-mail system needs to be a fortress filled with defenses.

- Don't use free web-based e-mail accounts for your business.
- Establish your own domain and create e-mail accounts based on that domain.
- Ensure that your firewalls, virus software, and spam filters are robust and up-to-date.
- Immediately report and delete suspicious e-mails, particularly those that come from people you don't know.
- If you receive an e-mail from someone who appears to be a legitimate contact; but you are wary, make sure you "forward" it back to the sender. Do not hit "reply." That way you can manually type the known e-mail address or find it in your established contact list to confirm authenticity.
- Don't click in a moment of panic. Fraudsters often use social engineering to stress you out so you will act quickly without thinking. Check before you click.
- Consider two-factor authentication for employee e-mail.
- Create a security system that flags e-mails with similar -- but incorrect -- formatting.
- Make sure your e-mail is encrypted in-transit if you are putting sensitive information into it.

Read the full FBI Tech Tuesday article [here](#).

The Dark Web.

C
y
b
e
r
.
s
i
d
e
.
C
h
a
t

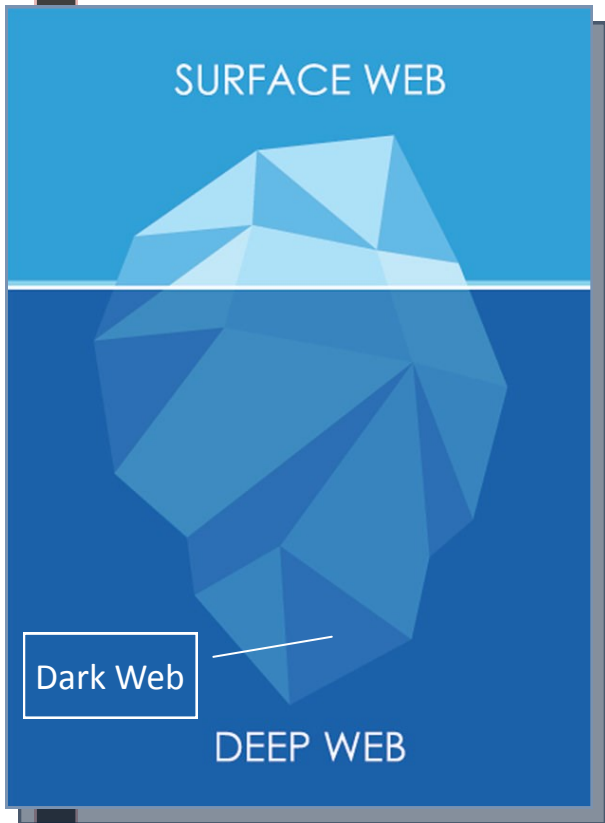
Often seen as a hacker's playground, popular shows referencing the dark web includes Mr. Robot and House of Cards. Regardless of its portrayed uses, some of which are most definitely true, the dark web does in fact exist but it is a little more complicated than that. This article provides an introductory lesson on the dark web and its uses.

SurfaceWeb + DeepWeb = WorldWideWeb

First, it is important to understand the scope and structure of this topic. To understand the internet's topology, imagine it as an iceberg. Similar to physical icebergs, the World Wide Web's size is misleading. What you see on the surface is not all of what you get. The surface web is all content indexable (searchable) and readily available through common web browsers or search engines such as Google, Bing, and [Duck-Duck-Go](#). Although the surface web appears large, it fails to compete with the uncalculatable size of the deep web hidden below the observable surface.



If the surface web contains all indexable internet content than the deep web as everything else. All deep web content is bound by a single principle; it is not indexable by popular browsers or search engines. Examples of common non-indexable content include private networks and web pages such as DPSNET; non-HTML or obscure file formats; and dynamic pages generated in response to a query. Much of this content is not accessible because login credentials or payment is required to proceed. In most cases, this barrier protects sites such as email servers or intellectual property from unauthorized access. It is safe to assume much of deep web content is not malicious; however, by definition, the deep web also includes traffic anonymizing networks such as Tor or Freenet and private Peer-2-Peer networks.



Understanding the Dark Web.

This part of the deep web is known as the dark web. Often incorrectly used as interchangeable terms, the dark web and deep web are different. Putting it simply, the dark web resides within the deep web. Returning to the iceberg model, the dark web is located below the surface internet but commands an extremely minimal portion of the deep web. Dark web software is special, because it produces high levels of anonymity for their users and websites. Using this anonymity mischief may be managed.

The dark web is notorious as a breeding ground for illegal services and content. Just to name a few, it has been used for terrorism, malicious hacking, and distributing child pornography. Some infamous hidden services to name include the Silk Road, Assassination Market, and of course,

[AlphaBay](#). Although many users utilize this technology to commit crimes; ultimately, it is the users that decided how and why to use the technology.

It is very important to understand that the dark web is not inherently evil, and has legitimate uses too. People often seek the privacy provided by the advanced cryptography of the dark net. In countries where mass surveillance is used to suppress populations or produce a chilling effect to restrict journalism, the dark web may be their only hope of reporting the real facts or fleeing to safety. Political revolutions are no stranger to the benefits of anonymity but the shield of justice depends on it. Witness protection programs or undercover investigations are relevant cases in which maintaining internet anonymity may be the deciding factor between life or death.

The debate over privacy and safety is age old and double-edged. Frankly speaking, that topic may never be settled. However, Cyber Security's goal is to help you learn something new with each publication and inspire personal research into security related topics. Because knowledge is power and understanding technology is the best defense against it.

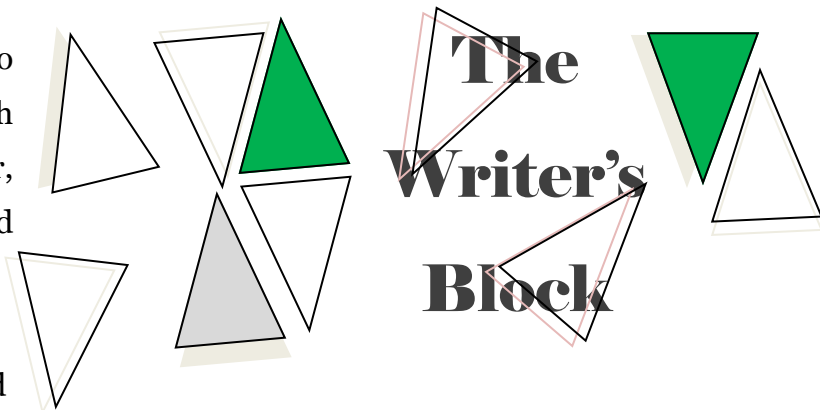
Introducing: Cyber Side Chats

I hope that the dark web article inspired you to embark on your own security research adventures and learn all the things! However, if iceberg diagrams cooled your interests, send me an [email](#) suggesting a new security topic to research, compare, and explain in the next “Cyber Side Chat”. Security is pretty cool, and

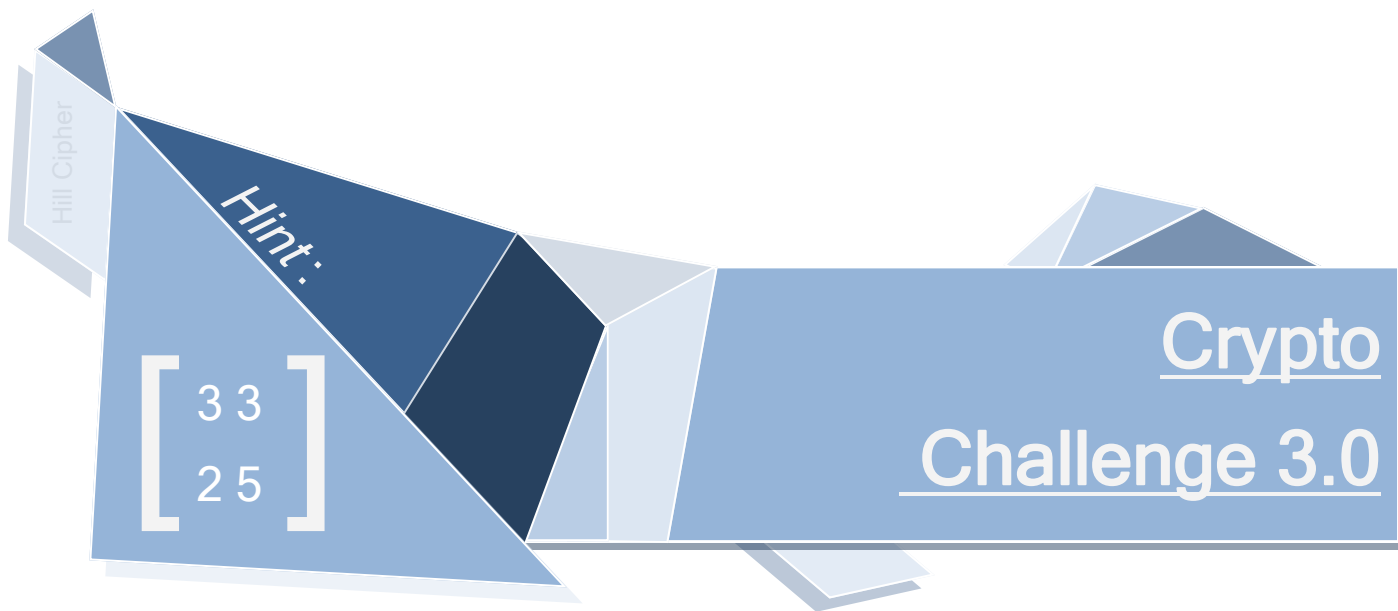
I want to engage you as much as possible. Together we can share information and expand our security knowledge.

Best,

J. G. Carson.



The Writer's Block



“QOFFSCUBOSLCBLVEJGRG”

Newsletter Support

GRP_Cyber_Risk@dps.texas.gov

Connect & Share

[Website](#) | [Twitter](#)