Security Newsletter

24 July 2017

Dark net markets AlphaBay and Hansa shut after huge international police sting

Earlier this month, news broke that authorities had seized the Dark Web marketplace AlphaBay, an online black market that peddled everything from heroin to stolen identity and credit card data.

But it wasn't until today, when the U.S. Justice Department held a press conference to detail the AlphaBay takedown that the other shoe dropped: Police in The Netherlands for the past month have been operating Hansa Market, a competing Dark Web bazaar that enjoyed a massive influx of new customers immediately after the AlphaBay takedown.

FBI Active Director McCabe said AlphaBay was ten times larger than Silk Road, with over 250,000 listings for illegal drugs and toxic chemicals; and over 100,000 listings for stolen and fraudulent identification documents and access devices, counterfeit goods, malware and other computer hacking tools, firearms and fraudulent services.

Read More

Even More

Microsoft Office 365 Users Targeted in Brute Force Attacks

Enterprise Office 365 accounts, many belonging to high-level employees at Fortune 2000 companies, were hit with a brute-force attack in one of the earliest operationalized cloud-to-cloud business attacks, according to Skyhigh Networks, which began tracking the campaign early this year.

Attackers tried logging in with different versions of employees' usernames, a sign they may have already possessed names and passwords but needed usernames for spearphishing campaigns or data access.

All login attempts came from instances hosted on cloud service platforms and targeted 48 businesses. **The "slow-and-low" pace of attacks indicates threat actors were trying to stay under the radar**; for each business, only a handful of senior employees were targeted. All those who were hit have been notified.

Read More

Initial report

Windows Kerberos security hole – the “Orpheus’ Lyre” attack explained

Orpheus' Lyre (OL) is a security hole in a venerable network authentication system called Kerberos, probably best known because it is widely used by Windows for logon and access control.

The Kerberos concept is much like the way train tickets work: the platform barriers that open to let you get on your train don’t need to be able to accept payments, issue tickets, give change, or help you select from the options available for your chosen journey; instead, they just need to know how to validate the ticket you already bought at a ticket machine or the ticket office.

According to the researchers who found the OL hole, this bug means that an attacker on your network could modify an official Kerberos reply in order to lure an unpatched client computer to an imposter server. To continue our train analogy, crooks could undetectably adjust Kerberos tickets to persuade client computers to travel trustingly all the way to EDINBURGH instead of getting off at EALING BROADWAY as originally intended.

The Windows implementation of Kerberos used to be vulnerable, but was fixed in Microsoft’s July 2017 security update under the designation CVE-2017-8495, so make sure you’ve installed the latest Windows patches. Also, numerous open source implementations, such as those in various Linux distributions, in the Samba networking software, and in FreeBSD, have been patched, so apply updates to affected open source Kerberos components as soon as you can.

Read More

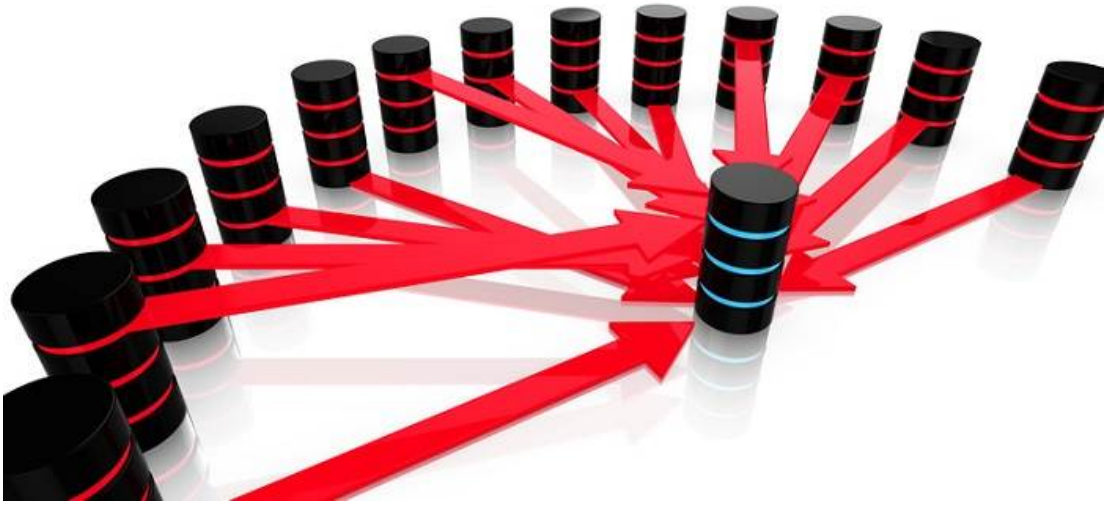
"Official" website

Android App Security Checklist

A checklist with security considerations for designing, testing, and releasing secure Android apps. It is based on the OWASP Mobile Application Security Verification Standard and Mobile Security Testing Guide. Follow the links on each checklist item for detailed instructions and recommendations.

Read More

How to DDoS Like an Ethical Hacker



You've just arrived home after a long work day. You wander a bit through the darkness, grab two slices of bread, and put them into that old, creaking toaster. The moment you push down on the button to toast the bread, you hear a loud pop, and all of the lights suddenly go out.

"Damn, the fuse blew up." Because the toaster was faulty, it flooded the electrical installation with excessive current it wasn't designed to handle. This blew up the fuse, and shut down the installation.

A nearly identical process takes place in DDoS attacks. Replace "electrical current" with "information", and "installation" with the term "information processor", and you've already understood the basic principle.

Read More

Millions of IoT devices hit by 'Devil's Ivy' bug in open source code library

A flaw in a widely-used code library known as gSOAP has exposed millions of IoT devices, such as security cameras, to a remote attack.

Researchers at IoT security firm Senrio discovered the Devil's Ivy flaw, a stack buffer overflow bug, while probing the remote configuration services of the M3004 dome camera from Axis Communications. The bug occurs when sending a large XML file to a vulnerable system's web server.

According to Senrio, as of July 1 there were about 14,000 Axis cameras exposed on the internet. But as the security firm notes, this bug "goes far beyond" Axis communications kit thanks to gSOAP's widespread use and will likely remain exposed on devices for a long time. Genivia counts Adobe, IBM, Microsoft, and Xerox as customers and claims gSOAP has been downloaded more than a million times.

Read More

Initial report

Humble bundle cybersecurity

Humble Bundle is offering a new collection of tech ebooks for cyber security enthusiasts, straight from the libraries at Wiley/Sybex. The Cybersecurity Book Bundle includes Secrets and Lies: Digital Security in a Networked World, Applied Cryptography: Protocols, Algorithms and Source Code in C, The Art of Deception: Controlling the Human Element of Security, Social Engineering: The Art of Human Hacking, and lots more!

Starting at 1$ for 4 books, you can get up to 14 books if you pay 15$ or higher.

The Humble Book Bundle concept is to offer numerous different bundles of books, available for a limited time at a pay-what-you-want price model. All of the offered ebooks are DRM-free. The Humble Bundle allows buyers to choose the payment amount and divide it among the editors, listed charities, and the Humble Bundle itself.

Read More

This content was created by Kindred Group Security. Please share if you enjoyed!

Kindred Group in brief

Kindred is one of the largest online gambling companies in the world with over 15 million customers across 100 markets. We offer pre-game and live Sports betting, Poker, Casino and Games through 13 subsidiaries and brands across our markets. We are committed to offer our customers the best deal and user experience possible, while ensuring a safe and fair gambling environment. Kindred is a pioneer in the online gambling industry and as an innovation driven company that builds on trust.