kindred

Security Newsletter

30 April 2018

Subscribe to this newsletter

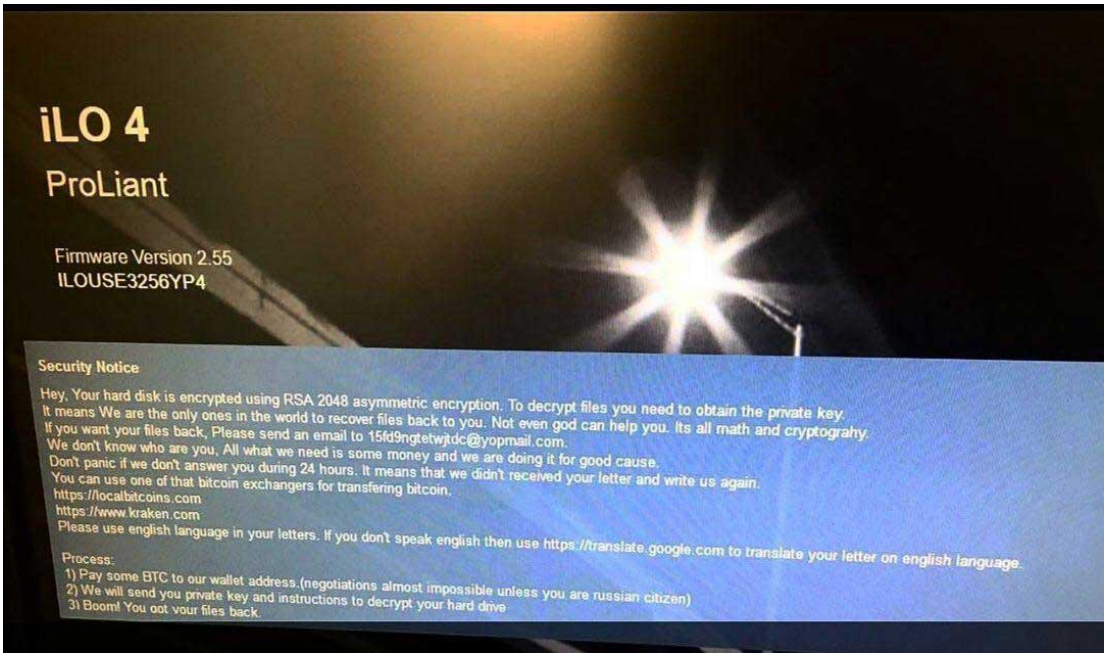
SEC Fines Yahoo $35 Million for Data Breach

The United States Securities and Exchange Commission has fined Yahoo $35 million for failing to disclose a massive security breach that took place in 2014. The fine is for the first Yahoo data breach that came to light in 2016 —the one where hackers stole the usernames, email addresses, phone numbers, birthdates, encrypted passwords, and security questions for over 500 million Yahoo users.

The fine comes after Yahoo filed its quarterly documents in November 2016, two months after announcing the first breach, admitting that it knew about the breach since 2014, and not 2016, when the breach became public. This meant that Yahoo leadership purposely hid the data breach.

Read More

Ransomware Hits HPE iLO Remote Management Interfaces



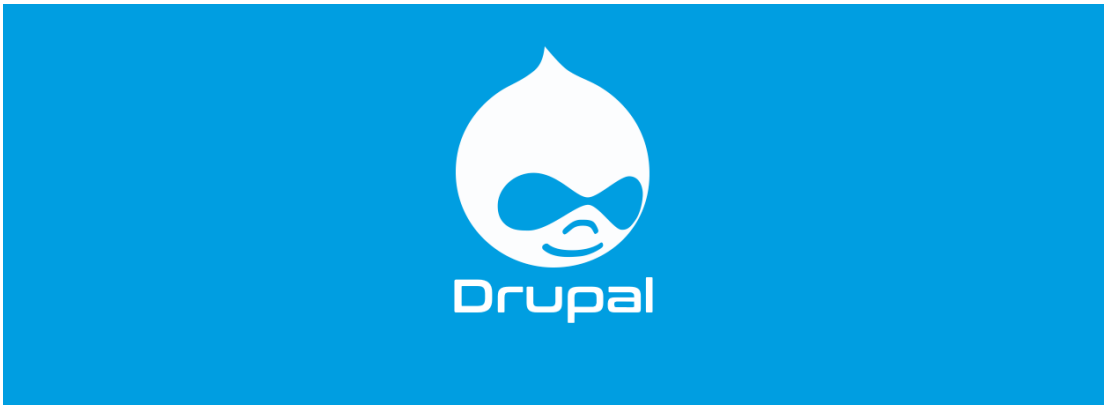
HPE iLO 4, otherwise known as HPE Integrated Lights-Out, is a management processor built into certain HP servers that allow administrators to remotely administer the device. Attackers are targeting Internet accessible HPE iLO 4 remote management interfaces, supposedly encrypting the hard drives, and then demanding Bitcoins to get access to the data again.

An interesting part of the ransom note is that the attackers state that the ransom price is not negotiable unless the victim's are from Russia. This is common for Russian based attackers, who in many cases tries to avoid infecting Russian victims.

Exposing a remote administration tool like iLO 4 to the Internet is never a good thing to do. These tools should only be accessible via secure VPNs in order to prevent them from being scanned for and accessed by anyone on the Internet. Finding connected iLO interfaces is also trivial. A quick search on Shodan shows that over 5,000 iLO 4 devices are connected to the Internet, with many of them being known vulnerable versions.

Read More

New critical Drupal Vulnerability already exploited in the wild



The new flaw that is being exploited is a remote code execution (RCE) bug that affects both Drupal 7.x and 8.x versions. The vulnerability was rated 19 out of 25 on Drupal's own severity scale ("Critical"), meaning it can give attackers complete control over an attacked site. After the detection of in-the-wild exploit only hours after the patch release, the vulnerability score was bumped to 20/25 ("Highly critical").

This vulnerability should not be confused with Drupalgeddon 2 (CVE-2018-7600), another Drupal CMS security issue patched last month, which is also heavily exploited. In a public announcement from mid-April, the Drupal Security team announced that websites that were not patched against Drupalgeddon 2 by the 11th of April may be considered as compromised.

Read More

Read Drupal Security Advisory SA-CORE-2018-004

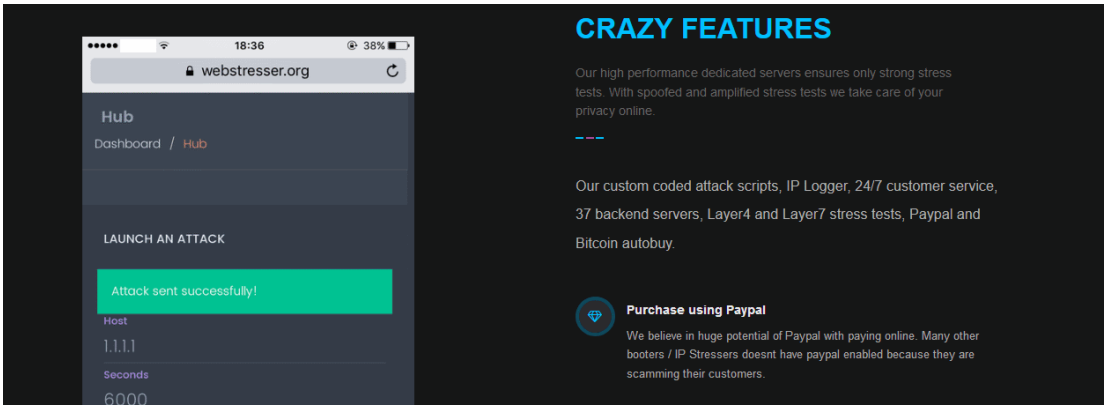
Millions Of Hotel Room Keys Can Be Hacked

F-Secure researchers Tomi Tuominen and Timo Hirvonen have found serious design flaws within Assa Abloy's smart lock system Vision by Vingcard, used in a massive number of hotels and other institutions around the world. When exploited, these issues allow a potential attacker to open any door within a facility that uses the lock system, and get access to its restricted areas.

The attack is simple: you need to get ahold of an electronic keycard that opens a lock within the target facility. Any key will work, active or inactive (think lost), whether it's used to open a highly-secure room or a broom closet. The attacker can then use a small electronic device to generate a master key and open all the doors within the target facility. The system of the electronic device will not be released by F-Secure.

Read More

Europol Shuts Down World's Largest DDOS-for-Hire Service



Europol officials have shut down WebStresser, a website where users could register and launch DDoS attacks after paying for a monthly plan, with prices starting as low as €15 ($18.25). The website, considered the largest DDoS-for-hire service online, had over 136,000 users at the time it was shut down. Europol said it had been responsible for over 4 million DDoS attacks in recent years.

Besides shutting down the website's server infrastructure, authorities said they also arrested the site's administrators, located in the United Kingdom, Croatia, Canada, and Serbia. Dutch and UK cops led the investigation and were responsible for tracking down administrators and their infrastructure. Cops seized WebStresser's server infrastructure located in the Netherlands, the US and Germany.

Not only did Europol arrest site administrators, but also they took "further measures" against the site's top users who have launched the most attacks in the recent years. Officials didn't reveal what these measures were but merely said the users were located in the Netherlands, Italy, Spain, Croatia, the United Kingdom, Australia, Canada and Hong Kong.

Read More

Cutting room floor

- How third-party trackers abuse Facebook Login to exfiltrate PII and track people
- Spoofing Cell Networks with a USB to VGA adapter
- How "Keen Security Lab" exploited VMware during the Pwn2Own 2017 competiton #VMEscape
- Fuzzing Adobe Reader for exploitable vulns
- Startup offers $3 Million to anyone who can hack the iPhone
- Cisco's Talos analysis of a cryptomining campaign
- Cisco's Talos uncovering of a new piece of malware

#Tech and #Tools

- Snallygaster, a tool to scan for secret files on HTTP servers
- PowerUpSQL, a PowerShell Toolkit for Attacking SQL Server
- A PoweShell script to interact with MITRE's ATT&CK Framework
- New Anti-VM trick discovered by a Cisco's Talos Analyst

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.