kindred

Security Newsletter

3 July 2017

52% of All JavaScript npm Packages Could Have Been Hacked via Weak Credentials

Tens of thousands of developers using weak credentials to secure their npm accounts inadvertently put more than half of the npm packages (JavaScript libraries and tools) at risk of getting hijacked and used to deploy malicious code to legitimate applications that use them in their build process.

npm Inc, the company that runs the npm package manager, has addressed the issue at the start of June by triggering password reset operations for all affected users.

Read More

WordPress Plugin Used by 300,000+ Sites Found Vulnerable to SQL Injection Attack

A SQL Injection vulnerability has been discovered in one of the most popular Wordpress plugins, installed on over 300,000 websites, which could be exploited by hackers to steal databases and possibly hijack the affected sites remotely.

The flaw has been discovered in the highly popular WP Statistics plugin, which allows site administrators to get detailed information related to the number of users online on their sites, the number of visits and visitors, and page statistics.

Read More

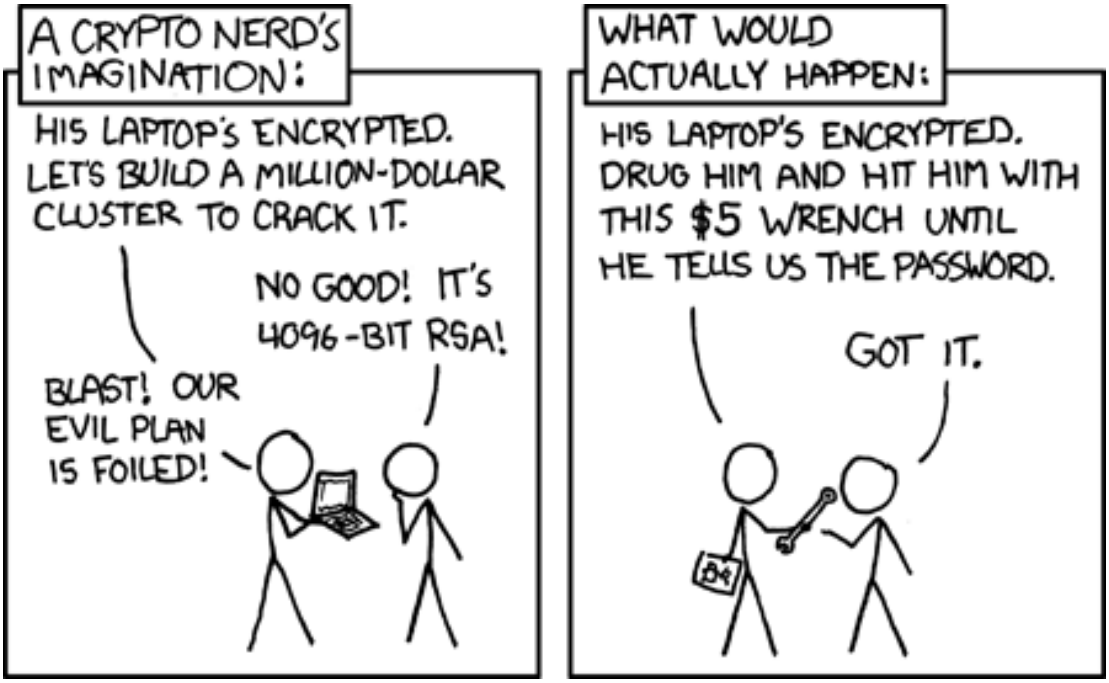
New ransomware, old techniques: Petya adds worm capabilities

On June 27, 2017 reports of a ransomware infection began spreading across Europe. We saw the first infections in Ukraine, where more than 12,500 machines encountered the threat. We then observed infections in another 64 countries, including Belgium, Brazil, Germany, Russia, and the United States.

The new ransomware has worm capabilities, which allows it to move laterally across infected networks. Based on our investigation, this new ransomware shares similar codes and is a new variant of Ransom:Win32/Petya. This new strain of ransomware, however, is more sophisticated.

Read More

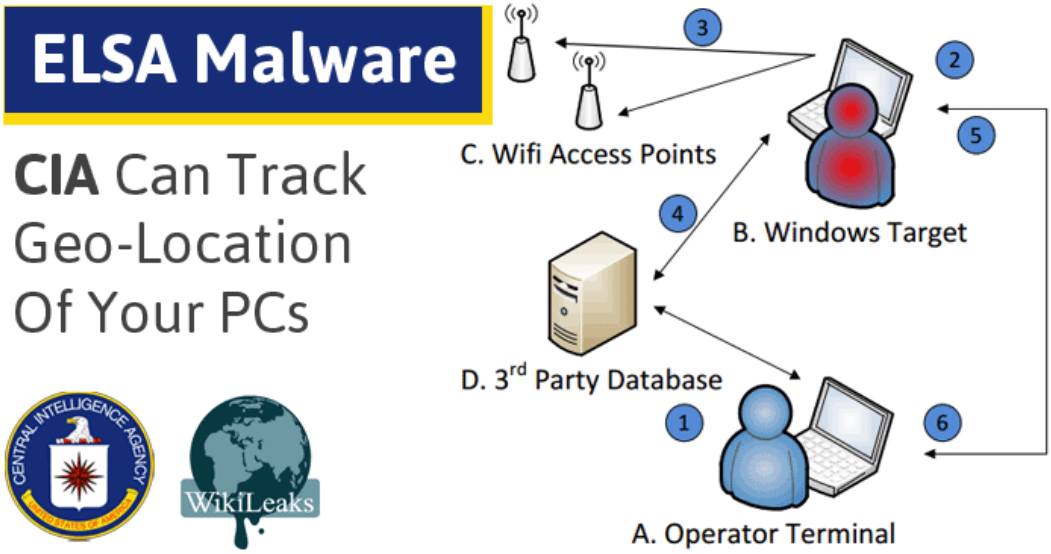
How Not to Encrypt a File—Courtesy of Microsoft



A client recently sent me a crypto spec which involved some, how do I say, suboptimal use of crypto primitives. They're .Net users so I decided to search for a nice msdn crypto reference to set them straight. Instead I found the likely culprit behind their confusion.

Read More

Vault 7: CIA Malware for Tracking Windows Devices via WiFi Networks



Today, WikiLeaks has published the documentation manual for an alleged CIA tool that can track users of WiFi-capable Windows devices based on the ESS (Extended Service Set) data of nearby WiFi networks.

According to the tool's 42-page manual, the tool's name is ELSA. The manual includes the following image to explain to CIA operatives how the tool works. A summary of an ELSA operation is included below the image.

Read More

OutlawCountry Is CIA's Malware for Hacking Linux Systems

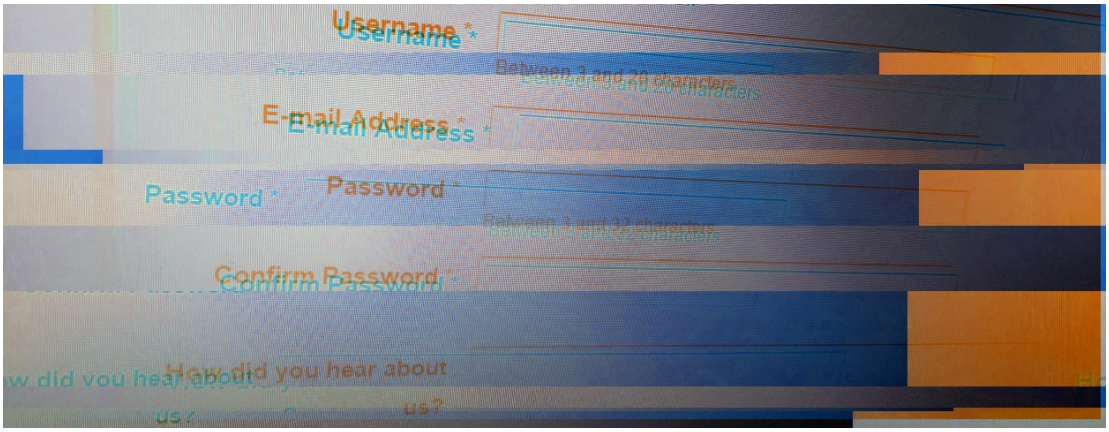
WikiLeaks dumped today a manual describing a new CIA malware strain. Called OutlawCountry, this is malware designed for Linux operating systems.

The leaked user manual — dated 04 June 2015 — details a kernel module for Linux 2.6 that allows CIA operatives to divert traffic from a Linux machine to a chosen destination.

Shell access and root privileges are needed to install OutlawCountry, meaning CIA operatives must compromise machines via other means before deploying this malware strain.

Read More

PRMitM: Attackers Can Hide Password Resets Inside Account Registrations



A research paper published by four Israeli scientists details a new attack called PRMitM, or the "Password Reset Man-in-the-Middle," in which attackers hide password reset interactions for a user's legitimate profile inside account registration interactions on another site.

The attack falls under the category of social engineering, as it requires an attacker to convince or lure a potential victim to register a profile on a boobytrapped website.

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.