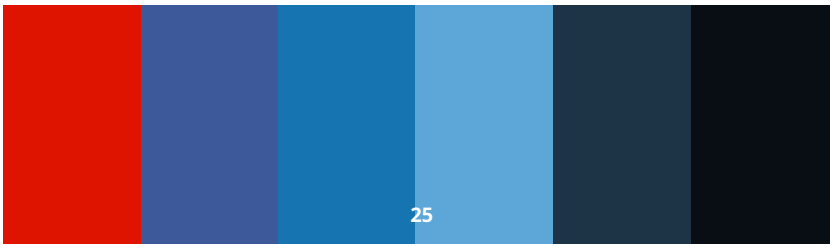
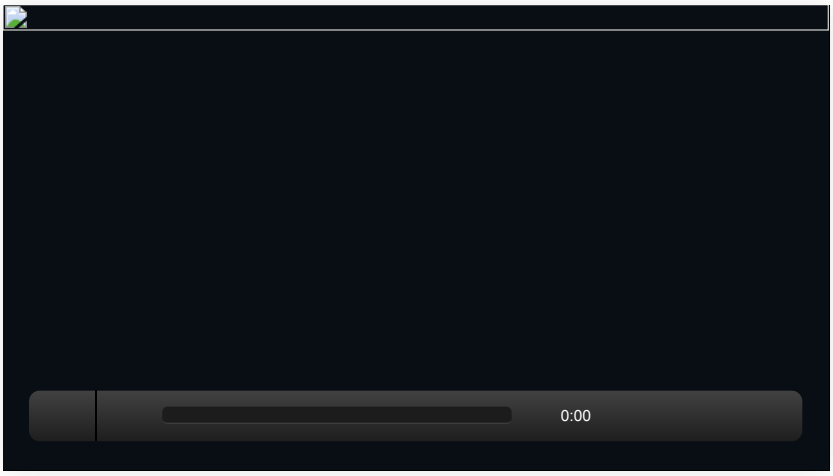
ALL WI-FI NETWORKS CAN NOW BE CRACKED WITH EASY TOOL - CANDIDATES BEWARE

New Wi-Fi attack cracks WPA2 passwords with ease

The common Wi-Fi security standard is no longer as secure as you think.

By Charlie Osborne for Zero Day | August 8, 2018 -- 08:40 GMT (01:40 PDT) | Topic: Security





A new way to compromise the WPA/WPA2 security protocols has been accidentally discovered by a researcher investigating the new WPA3 standard.

The attack technique can be used to compromise WPA/WPA2-secured routers and crack Wi-Fi passwords which have Pairwise Master Key Identifiers (PMKID) features enabled.

Security researcher and developer of the Hashcat password cracking tool Jens "Atom" Steube made the discovery and shared the findings on the Hashcat forum earlier this month.

At the time, Steube was investigating ways to attack the new WPA3 security standard. Announced in January by industry body the Wi-Fi Alliance, WPA3 is the latest refresh of the Wi-Fi standard.

MORE SECURITY NEWS

- **Iran cited as growing threat in cybersecurity landscape**
- **Fizzing up the new TLS security protocol**
- **Salesforce warns customers of data leak caused by API error**
- **IoT security warning: Your hacked devices are being used for cybercrime says FBI**

WPA3 aims to enhance user protection, especially when it comes to open Wi-Fi networks and hotspots commonly found in public spaces, bars, and coffee shops. The new standard will utilize individualized data encryption to scramble connections -- as well as new protections against brute-force attempts to crack passwords.

However, the aging WPA2 standard has no such protection.

According to the researcher, the new attack method does not rely on traditional methods used to steal Wi-Fi passwords. Currently, the most popular method is to wait until a user connects to Wi-Fi, wait for the four-way authentication handshake to take place, and capture this information in order to brute-force the password in use.

See also: Disclose.io: A safe harbor for hackers disclosing security vulnerabilities

Instead, the new technique is performed on the Robust Security Network Information Element (RSN IE) of a single EAPOL frame.

The attack is clientless and does not require regular users to be involved at any stage. Information gathered is translated in regular hex encoded strings, which means that no special

translation or output formats will thwart attackers or cause delays.

TechRepublic: **Happy World Wi-Fi Day: Here are 5 best practices for good home network hygiene**

If a Wi-Fi network is compromised through the technique, cyberattackers may be able to steal pre-shared login passwords, eavesdrop on communications and perform Man-in-The-Middle (MiTM) attacks.

"At this time, we do not know for which vendors or for how many routers this technique will work, but we think it will work against all 802.11i/p/q/r networks with roaming functions enabled (most modern routers)," Steube says.

CNET: **Best Wi-Fi Systems for 2018**

WPA3 is due to be released en masse this year, and once the protocol becomes firmly established, it will be far harder across the board for cyberattackers to compromise Wi-FI systems in order to extract passwords.

The attack will not work against WPA3, as Steube says it will be "much harder to attack because of its modern key establishment protocol," the use of "Simultaneous Authentication of Equals" (SAE).