On July 25, 2019, the Cyber Threat Alert Level was evaluated and is remaining at Blue (Guarded) due to multiple vulnerabilities in Apple products.

Threat Level's explained

- **GREEN or LOW** indicates a low risk.
- **BLUE or GUARDED** indicates a general risk of increased hacking, virus, or other malicious activity.
- **YELLOW or ELEVATED** indicates a significant risk due to increased hacking, virus, or other malicious activity that compromises systems or diminishes service.
- **ORANGE or HIGH** indicates a high risk of increased hacking, virus, or other malicious cyber activity that targets or compromises core infrastructure, causes multiple service outages, causes multiple system compromises, or compromises critical infrastructure.
- **RED or SEVERE** indicates a severe risk of hacking, virus, or other malicious activity resulting in widespread outages and/or significantly destructive compromises to systems with no known remedy or debilitates one or more critical infrastructure sectors.

WEEKLY IT SECURITY BULLETIN

02 August 2019

In The News This Week

Capital One Data Theft – One of the biggest data breaches ever!

In one of the biggest data breaches ever, a hacker gained access to more than **100 million** Capital One customers' accounts and credit card applications earlier this year.

Paige Thompson is accused of breaking into a Capital One server and gaining access to 140,000 Social Security numbers, 1 million Canadian Social Insurance numbers and 80,000 bank account numbers, in addition to an undisclosed number of people's names, addresses, credit scores, credit limits, balances, and other information, according to the bank and the US Department of Justice. A criminal complaint says Thompson tried to share the information with others online. The 33-year-old, who lives in Seattle, had previously worked as a tech company software engineer for Amazon Web Services, the cloud hosting company that Capital One was using. Thompson was arrested Monday in connection with the breach, the Justice Department said. Thompson's attorney could not be immediately reached for comment.

Capital One (COF) said the hack occurred March 22 and 23 and includes credit card applications as far back as 2005. The company indicated it fixed the vulnerability and said it is "unlikely that the information was used for fraud or disseminated by this individual." However, the company is still investigating. "I sincerely apologize for the understandable worry this incident must be causing those affected and I am committed to making it right," said Capital One CEO Richard Fairbank in a statement.

The breach affected around 100 million people in the United States and about 6 million people in Canada, according to Capital One. However, "no credit card account numbers or log-in credentials were compromised and over 99% of Social Security numbers were not compromised," the company noted.

Capital One said it will notify people affected by the breach and will make free credit monitoring and identity protection available. The company expects to incur between $100 million and $150 million in costs related to the hack, including customer notifications, credit monitoring, tech costs and legal support due to the hack. Capital One's stock was down 5% in premarket trading Tuesday.

How Capital One got hacked - The criminal complaint against Thompson paints a picture of a less-than-careful suspect. Thompson posted the information on GitHub, using her full first, middle and last name, the complaint says. She also boasted on social media that she had Capital One information. In a channel on Slack, a chat service often used by businesses as well as other groups, Thompson explained the method she used to break into Capital One. She claimed to use a special command to extract files in a Capital One directory stored on Amazon's servers. "I wanna get it off my server that's why I'm archiving all of it lol," Thompson allegedly posted on Slack. One person was alarmed by what Thompson found, writing that the information was "sketchy," adding, "don't go to jail plz." Thompson made little effort to disguise her identity. She allegedly used the screen name "erratic" on Slack, which was the same handle she used on a Twitter account and a Meetup chatroom page.

The FBI special agent who investigated Thompson believes Thompson tweeted that she wanted to distribute Social Security numbers along with full names and dates of birth. One person who saw the information on GitHub notified Capital One of the "leaked data" belonging to the company. Capital One notified the FBI, and an agent searched Thompson's residence on Monday. They found devices in her possession that reference Capital One and Amazon as well as other entities that may have been targets of attempted — or actual -- breaches. The complaint indicates Thompson "recognizes that she has acted illegally." Read the full story here: CNN Business

Dealing with NIST's about-face on password complexity

In the last few years, we've been seeing some significant changes in the suggestions that security experts are making for password security. While previous guidance increasingly pushed complexity in terms of password length, the mix of characters used, controls over password reuse, and forced periodic changes, specialists have been questioning whether making passwords complex wasn't actually working against security concerns rather than promoting them.

Security specialists have also argued that forcing complexity down users' throats has led to them writing passwords down or forgetting them and having to get them reset. They argued that replacing a password character with a digit or an uppercase character might make a password look complicated, but does not actually make it any less vulnerable to compromise. In fact, when users are forced to include a variety of characters in their passwords, they generally do so in very predictable ways. Instead of "password", they might use "Passw0rd" or even "P4ssw0rd!", but the variations don't make the passwords significantly less guessable. People are just not very good at generating anything that's truly random.

The other argument that's been made is that putting the onus of generating and using complex passwords on the heads of the end users leaves them with a lot of stress and responsibility that might be better handled in some other way.

These changes in password composition recommendations have been coming at us for a while – generally in articles or posts about how setting overly strict password complexity standards might actually be making accounts less safe. Still, it's only been since NIST's fairly recent draft of its Special Publication 800-63-3: Digital Identity Guidelines (https://pages.nist.gov/800-63-3/) that those of us who manage servers have really begun to feel the need to sit back and pay attention. What do the rule changes mean to us? What might we do differently?

While these guidelines primarily apply to government agencies, the same guidance will likely work its way into companies who work with government agencies, have government customers, or simply want to adhere to what is likely to soon be considered best practice.

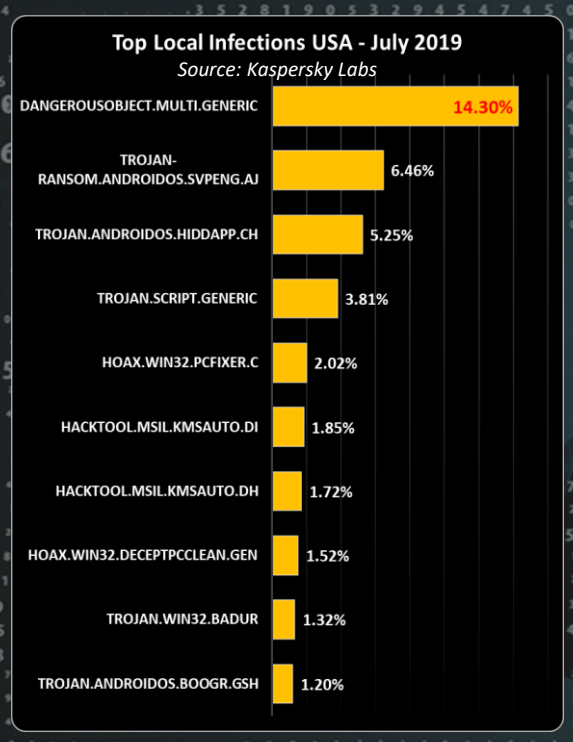
The new NIST guidance on passwords suggests that:

- passwords never expire
- no required character complexity or variety rules be implemented
- the maximum length for passwords be set to 64 characters
- the minimum length for passwords be set to 8 characters
- passwords be checked against known bad passwords, banned lists, etc.
- no hints or knowledge-based questions be provided to someone trying to log in (like "Who was your best friend in high school?")
- passwords only be changed when forgotten

As for minimum password length, the suggestion doesn't mean that you shouldn't consider setting your minimum password length to greater than 8 characters. I would still go with requiring 12-16 characters, especially if you remind your users that passwords can be fairly arbitrary and still be memorable. A phrase that they can remember like "Can I go home now?" or even "Ineedmorecoffee!" would work. You can also encourage your users to use truly random passwords -- like those generated by some of the password safe products. Passwords don't have to be easy to remember if they are cut and pasted as needed. The key to this strategy, however, is that they never forget the key to the safe.

Of course, the new guidance is not simply a relaxation of all constraints on passwords. The intent is to move away from complexity that doesn't improve security to complexity that does.

Adapted from an article by Sandra Henry-Stocker which you can find here: NetworkWorld



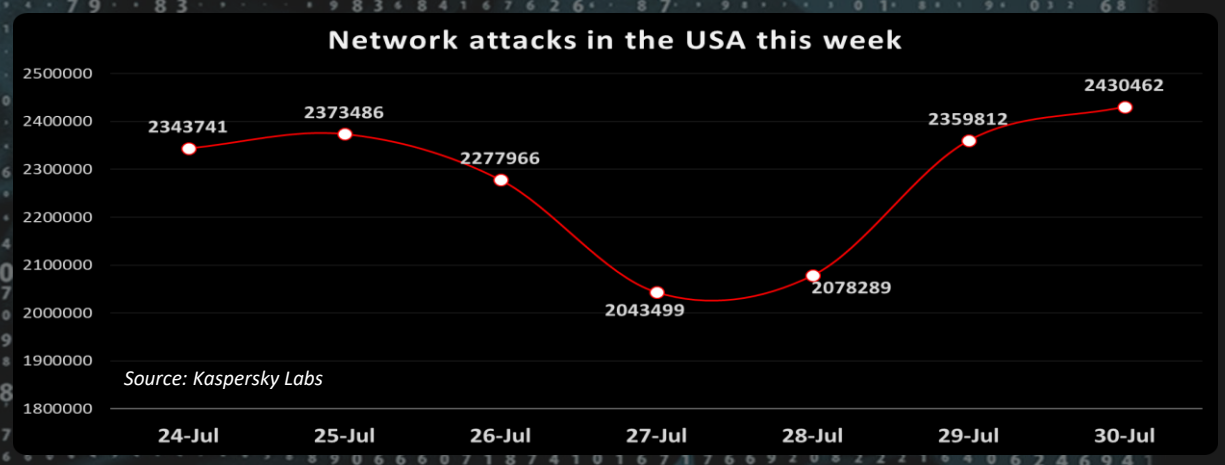
For Reporting Cyber Crime go to the Internet Crime Complaint Center (IC3) www.ic3.gov

Average time to crack a password (Measured by character length of password vs a brute force crack method)

Length	Time to crack
7 -	.29 milliseconds
8 -	5 hours
9 -	5 days
10 -	4 months
11 -	1 decade
12 -	2 centuries

CLICK HERE TO CHECK IF YOUR EMAIL ADDRESS HAS BEEN COMPROMISED IN A DATA BREACH

"Have I Been Pwned?"



Author: Chris Bester
chris.bester@yahoo.com