Cyber News You May Not Hear

January 2020
Colorado Town Wires Over $1 Million to BEC Scammers
BleepingComputer, 3 Jan 2020:
Colorado Town of Erie lost more than $1 million to a business email compromise scam (BEC) that ended with the town's employees sending the funds to a bank account controlled by scammers. BEC (otherwise known as Email Account Compromise) is a type of financial fraud through which crooks deceive an organization's employee via computer intrusion or by using social engineering into wiring out funds to attacker-controlled bank accounts. The fraudsters used an electronic form on the town's website to request a change to the payment information on the building contract for Erie Parkway Bridge awarded to SEMA Construction in October 2018. "Specifically, the change was to receive payments via electronic funds transfer rather than by check," Erie Town Administrator Malcolm Fleming said in an email memo according to The Denver Post.

This resulted in the payment information used to wire roughly $1.01 million to SEMA on October 25, 2019, pointing to the attackers' accounts. "Once the payments were in that account, the perpetrators of this fraud sent the money via wire transfer out of the country".
Austria's Foreign Ministry Gets Hit by 'Serious Cyberattack'
CyWare, 6 Jan 2020:
Austria's foreign ministry faced a cyberattack on its information system in the late hours of Saturday, January 4, 2020. Based on the gravity and nature of the attack, officials believe that it might have been carried out by a "state actor." As a matter of coincidence, the attack came on the same day when Austria's Greens nodded to go-ahead for a coalition with the country's conservatives, the People’s Party, at a congress in Salzburg. Other European countries have fallen victim to similar attacks in the past. The German government's IT network experienced a serious cyber-attack in March 2018. However, last year, the EU acquired powers to punish those outside the block who launch cyberattacks on hospitals and banks, sway elections, and steal company secrets or funds.
2020 outlook for cybersecurity legislation

CSO, 6 Jan 2020: A number of bills have been passed by either the House or the Senate and are awaiting further action. Notable pieces of digital security-related bills that the House has passed include:

- R.2331 - SBA Cyber Awareness Act
- R. 1 - For the People Act of 2019.

A number of bills have been introduced or moved in either House or Senate committees and are likely candidates for further movement.... Among them are:

- R.4237 - Advancing Cybersecurity Diagnostics and Mitigation Act.
New phishing email campaign impersonates US postal service to deliver malware

(1 of 2)

Tech Republic, 14 Nov 2019: A new phishing campaign that's been touring Europe has now been hitting the United States with the goal of spreading a trojan onto computers, as detailed in a report released on Thursday by Proofpoint. On Nov. 12, 2019, Proofpoint researchers observed thousands of emails trying to deploy malicious Microsoft Word attachments in the US, according to the report. The emails impersonated messages from the United States Postal Service and were part of a campaign to infect systems with the IcedID banking trojan. Discovered in 2017 by IBM X-Force Research, IcedID typically targets banks, payment card providers, and other financial institutions in an attempt to steal user credentials. Instead of targeting financial companies, the campaign found by Proofpoint was heavily directly at the healthcare industry. The emails discovered use the URL uspsdelivery-service.com, while the malicious Word documents contain a purported RSA SecurID key. Opening the Word document triggers a Microsoft Office macro that launches a PowerShell script, which then downloads and installs IcedID onto the computer. The US is only the latest target in this new campaign, according to the report. In October and then again in November, Proofpoint observed the same threat actor, named internally as TA2101, aiming at businesses in Germany with emails impersonating the German Federal Ministry of Finance. Beyond the phony branding, the emails use .icu domains in the sender's address. In this case, the person behind the campaign chose to use Cobalt Strike. Commercially available as a licensed software tool typically used for penetration testing, Cobalt Strike has been coopted by cybercriminals to deploy malware. Sent primarily to German IT services companies, the fraudulent email promises a 2019 tax refund, asking the recipient to open an attached Word document to submit a claim for the refund. Instead, opening the document launches an Office macro that executes a PowerShell script, which then downloads and installs Maze ransomware. Later in October, Proofpoint found a similar campaign running in Italy.
What you need to know about the Microsoft Windows 10 patch

USA Today, 16 Jan 2020: Microsoft has released a patch for its Windows 10 operating system to fix a major vulnerability that could expose users to breaches or surveillance. The National Security Agency alerted the software giant to the flaw in Windows 10, which is the most widely used operating system. Organizations and companies running Windows 10 should implement the patch immediately, Anne Neuberger, the director of the NSA’s Cybersecurity Directorate, told reporters Tuesday. The Department of Homeland Security recommended isolating systems that cannot be updated. Microsoft confirmed that a security update was released Tuesday. It also said that its security software can detect and block malware attempting to exploit the vulnerability.

Microsoft says the flaw was in the digital signatures used to determine if software is authentic, one of the ways that software makers work to prevent malware or spyware cloaked as legitimate software. The NSA discovered a mistake in how Microsoft verified signatures, which hackers could have exploited. "This vulnerability is one example of our partnership with the security research community where a vulnerability was privately disclosed and an update released to ensure customers were not put at risk," Microsoft said.
Microsoft ends free Windows 7 security updates on Tuesday
Associated Press, 13 Jan 2020: If you're still using Microsoft's Windows 7, your computer might soon be at risk. Microsoft will stop providing free security updates for Windows 7 on Tuesday (14 Jan), meaning computers using it will be more vulnerable to malware and hacking. Users who want to protect their computers need to upgrade to Windows 10. They may also need to buy new computers because older machines might not be compatible with Windows 10. Tech companies typically phase out older systems after a number of years and focus efforts on updating current versions of software. Windows 7 came out in 2009. Windows 8, which came out in 2012, will have free support end in 2023. Microsoft is also ending support Tuesday for Windows Server 2008 or 2008 R2 operating systems. Those who run Windows 7 Professional or Windows 7 Enterprise can buy extended protection for up to three years. Microsoft will also be ending support on Oct. 13 for Office 2010 a package that includes word processing and spreadsheet software.