The Beacon

Florida Fusion Center #15-046 | Cyber and Critical Infrastructure Report | April 2015 Issue #6

Summary

On the Dangers of Bloatware — All devices come equipped with pre-installed software, or bloatware. It isn't all bad, but what are the risks?

Net Neutrality: What It Is, and Why You Should Care — Net neutrality is a buzz phrase in the news recently. What is its impact on Internet users?

CyberCaliphate and ISIL's Spread of Online Propaganda — How the Islamic State of Iraq and the Levant (ISIL) are spreading their message using social media.

Industrial Control Systems Pose Under-Appreciated Threat — We usually think of malware as a tool to steal information, but what happens when it's used to target industrial systems to cause physical damage?

Recently Observed Upatre Malware & Associated Phishing Campaign— This regularly updated and self-deleting Trojan horse malware is a sophisticated tool used in phishing campaigns. It's designed to be difficult for antivirus programs to detect.

Trends in Ransomware — Combining the anonymity of bitcoins with the tendency for users to be forgetful with their security practices, ransomware appears to be the malware of the future.

Contents

About *The Beacon*

The Secure Florida Beacon is published by Secure Florida to highlight cyber and critical infrastructure security information and awareness.

Secure Florida is an Internet safety and awareness effort of the Florida Department of Law Enforcement's Florida Infrastructure Protection Center (FIPC). The FIPC was established in 2002 to anticipate, prevent, react to, and recover from acts of terrorism, sabotage, cyber crime, and natural disasters. The FIPC is a team of cyber intelligence and critical infrastructure protection analysts. FIPC analysts work to protect Florida's infrastructure through FDLE's Internet safety and awareness effort (Secure Florida), and the website SecureFlorida.org.

If you see a topic where you would like more detailed reporting, or have seen something you think we need to know about, Let Us Know.

We welcome your feedback.
www.survemonkey.com/s/TheSFBeacon6

Contact SecureFlorida.org at:
(850) 410-7400
Admin@SecureFlorida.org

Editor's Corner

On The Dangers of Bloatware

'Bloatware' is a popular term to describe unnecessary software that comes pre-installed on devices. You have probably noticed when you buy new devices that many times there is already a lot of software already on it. Unfortunately, often it cannot be uninstalled. It will stay on the device and even run in the background, using valuable system resources.

Why do manufacturers install bloatware? Simply stated, because they get paid to do it. Bloatware can appear as antivirus programs that want you to pay for an upgrade, free games (that are filled with advertisements), "free" programs (that are not actually free), or smartphone apps touting premium services offered by your cellphone provider.

This is an issue for the user for a few reasons, and while some are simply pesky, some are downright dangerous to your device's security. One obvious annoyance is that they may persuade you to purchase programs you do not actually need (or even want). They also may take up a lot of hard drive space. Some of these issues are easily remedied and of little consequence, however the most dangerous bloatware compromises the security of your device.

Lenovo Superfish is one of the dangerous types. Computer manufacturer Lenovo pre-installed Superfish adware onto its laptops, and it was not immediately obvious to those who purchased them. However, the scary part was that this adware would track a user's web searches so that it could then insert third party ads on websites. In order to accomplish this, the adware included a self-signed root certificate that compromised the encryption built into the browser, making the computer vulnerable to a "man-in-the-middle" (MITM) attack. As we have discussed in previous issues, MITM attacks allow a third party to monitor and intercept your Internet traffic without detection, stealing bank account information, passwords, or other sensitive information. The Department of Homeland Security thought this vulnerability severe enough to issue an alert on the topic.

It is important when you get a new computer, tablet, smartphone, or other device that you take a look at all the programs already loaded onto it, and consider uninstalling or disabling any features that you do not want or need. This step could be what keeps your new device from running unnecessarily slowly, or even compromising your security.

For More Information:

DHS US-CERT Superfish Alert: https://www.us-cert.gov/ncas/alerts/TA15-051A

Lenovo Statement on Superfish: http://news.lenovo.com/article_display.cfm?article_id=1929

Lenovo Superfish Removal Tool: http://support.lenovo.com/us/en/product_security/superfish_uninstall

Secure FLORIDA.org
Florida Department of Law Enforcement
Florida Fusion Center
Florida Infrastructure Protection Center

Let Us Know:
(850) 410-7645
Admin@SecureFlorida.org

Cyber Highlights

Cyber Highlights represent issues cyber analysts have seen active in Florida. The following articles are intended to serve as overviews of issues we feel the citizens of Florida would benefit from knowing.

Contents

Net Neutrality: What it is, and Why You Should Care

What is it?

Net neutrality is a principle that guides how to treat data moving across the Internet. Under the rules of net neutrality, all information on the Internet must be treated equally in terms of speed, regardless of website, content, user, or owner of the data. This means that data from some websites cannot be cherry-picked to travel at faster speeds to consumers than from other sites.

The crux of the recent debate is that under current U.S. law, Internet Service Providers (ISPs) could create "fast lanes" and "slow lanes" for Internet traffic. This would mean that ISPs could filter traffic and slow down or speed up the time it takes for information to get to consumers based on content or even how much one pays for their Internet subscription. It would also allow ISPs to restrict what content even gets to consumers, effectively creating censorship of information.

There has been a lot of debate in recent years over this concept. In 1996, the U.S. Congress passed the Telecommunications Act, which required the Federal Communications Commission (FCC) to treat network owners as "common carriers," just like telephone communication, which meant that they could not block or discriminate against content to or from Internet users' computers.[1]

However, the FCC in recent years has treated Internet service as an information service rather than a telecommunications service. This gave broadband providers such as Comcast or Verizon a

Summary

The 400-page document released by the FCC boils down to three major points:[2]

- **Blocking:** ISPs may not block consumer access to legal content, applications, or services.
- **Throttling:** ISPs may not impair or degrade lawful Internet traffic on the basis of content, applications, or services.
- **Paid Prioritization:** ISPs may not favor some Internet traffic over other lawful traffic in exchange for any kind of special considerations. This means that ISPs are prohibited from creating "fast lanes" that allow certain website traffic to get to consumers faster in exchange for paying higher fees to ISPs. Likewise, ISPs cannot choose to prioritize any web-based content over others.

loophole to filter content and 'throttle' speeds for certain websites or users, i.e. purposely speeding up or slowing down one's access to specific sites or data. This meant that ISPs were ultimately the ones making the rules about how to deliver Internet traffic to consumers.

Why should consumers care?

In late February, the FCC released a ruling that classified ISPs as public utilities, a landmark decision that places Internet use in a category alongside those businesses responsible for providing the public with necessities such as water, electricity, and telephonic communication. In short, this ruling keeps ISPs from auctioning off faster traffic speeds for higher prices, or from blocking consumer access to sites that the ISPs don't like.

In late March, the first ISPs filed a lawsuit against the FCC, arguing that the new regulation of Internet as a utility is legally unsustainable. Over the coming months, there will probably be more lawsuits filed by other ISPs.

However, as FCC Chairman Tom Wheeler argued, these regulations are necessary in order to ensure that the Internet remains "fast, fair and open."[3]

[1] http://www.savetheinternet.com/net-neutrality-what-you-need-know-now

[2] https://nakedsecurity.sophos.com/2015/03/16/full-rules-for-protecting-net-neutrality-released-by-fcc/

[3] http://www.washingtonpost.com/blogs/the-switch/wp/2015/02/26/the-fcc-set-to-approve-strong-net-neutrality-rules/

CyberCaliphate and the Spread of Online Propaganda

In recent months, the criminal hacker group "CyberCaliphate," who claims affiliation with the Islamic State of Iraq and the Levant (ISIL), have conducted a series of cyber attacks. Their tactics are consistent with those of the average criminal hacker, but CyberCaliphate conducts these disruptive attacks in order to spread Islamist propaganda across the Internet. They engage in defacement of various government and Western websites using open source tools that only require basic technical capabilities.

Some recent incidents perpetrated by CyberCaliphate include:

- The targeting of a U.S. Marine's wife by hacking her Twitter account
- Hijacking the Twitter feed of Newsweek to publish intimidating messages
- Defacing Malaysia Airlines' website and posting a link leading to a passenger flight booking from the airline's internet email system

They also claim to have successfully infiltrated U.S. government databases, obtaining sensitive or even classified information. However, it appears the "stolen" information was obtained through "Google dorking," an advanced search technique that attempts to retrieve sensitive data residing on the Internet but not retrievable via normal web searches.

SecureFLORIDA.org
Florida Department of Law Enforcement
Florida Fusion Center
Florida Infrastructure Protection Center

LET US KNOW:
(850) 410-7645
Admin@SecureFlorida.org

The most notable recent incident occurred on January 12, 2015, when CyberCaliphate accessed and defaced the Twitter and YouTube accounts of the U.S. Central Command (CENTCOM). The hackers posted a series of threatening messages and screenshots of documents they claim were obtained by hacking the network of the U.S. military. CENTCOM issued a press release that these were false claims and no information released by the group came from CENTCOM servers or social media sites. Although a high profile attack, the methods utilized by the CyberCaliphate were not particularly complex.

The actors behind the CENTCOM attack are believed to be the same individuals who compromised media sites in December 2014 and January 2015. Affected organizations include the Albuquerque News Journal, WBOC 16 News in Maryland, and the Mountain View Telegraph based out of New Mexico. The propaganda image at the beginning of this article was posted by CyberCaliphate as part of their web defacement campaign.

To assist the private sector community, CENTCOM published a technical information paper (TIP-12-298-01) outlining useful practices for safeguarding public facing websites. This report can be found at:

http://www.us-cert.gov/security-publications/website-security.

Industrial Control Systems Pose Under-Appreciated Threat

The public has a certain idea in mind when they hear about data breaches. There is an image propagated by Hollywood of hackers in hoodies behind screens illuminated by lines of binary code, stealing information, accompanied by a fear that you may somehow end up a target.

However, the public perception of these risks grows less abstract with each data breach that appears in the news. The breach of Home Depot's payment system in 2014 cost the company roughly $43 million. Although 56 million customers had their payment information stolen, no one suffered any great loss, and more importantly, no consumer suffered any physical injury.

However, what could happen because of the vulnerabilities intrinsic, not in information technology, but in *operations technology*? Operations technology uses networked computers to control things that move: real, physical, and often moving parts such as motors, pumps, electricity, and air conditioners. How does risk in operations technology differ, since many of the same components and technologies exist in both realms? Every day increasing numbers of the components that control the machines we depend on connect to the Internet, some as indirectly as Home Depot's payment system.

If a system protected as well as Home Depot's payment system can be so readily breached, what is to stop a determined adversary from attempting a similar attack against components essential to operations technology? If a properly motivated attacker breaches an ICS (industrial control systems) component with some specifically designed malware, what is the potential cost? ICS components often run in remote locations and with little need of attention until something goes wrong.

As we discussed in the last issue of this publication, there is evidence nefarious actors have increasingly targeted ICS components. In December 2014 the U.S. Department of Homeland Security Industrial Control Systems Cyber Emergency Response Team (we'll stick with ICS-CERT from here on out) issued an alert about an ongoing sophisticated malware

Secure FLORIDA.org
Florida Department of Law Enforcement
Florida Fusion Center
Florida Infrastructure Protection Center

Let Us Know:
(850) 410-7645
Admin@SecureFlorida.org

campaign focused on compromising ICS components known as human machine interfaces, or HMIs.[1] HMIs are computer programs that allow technicians to interact with control equipment.

Similar technology can be used in your home, such as a thermostat that you control via smartphone. In an industrial environment, the consequences are even more dire. As such, ICS-CERT requests that owners and operators of ICS equipment survey their systems for components targeted by this particular malware campaign. If you are an owner or operator of any type of ICS equipment, please read the alert if you have not already.

Physical barriers will not hide ICS equipment from exploit. As more ICS components connect to computers and standard computer networks, its attack surface grows. Even Google can now find improperly configured ICS equipment.[2]

Owners of ICS equipment must recognize a broad range of potential threats whether it is an adversarial nation state, hacktivist, or some haphazard nonsense at the hands of a curious teen. Conside this: in 2008, a 14-year-old Polish boy modified a television remote control such that he could switch the tracks on the city tram in Lodz, Poland. He essentially commandeered the largest train set he could find and in the process caused a train to derail, injuring several passengers. Luckily, no one died. And this was only one curious, albeit misguided, boy.

The public increasingly perceives the risks associated with information breaches, but we must work to increase awareness on the other dangers that exist as technology becomes more vital to all parts of life.

1 Alert (ICS-ALERT-14-281-01B); Ongoing Sophisticated Malware Campaign Compromising ICS (Update B); Original release date: December 10, 2014; https://ics-cert.us-cert.gov/alerts/ICS-ALERT-14-281-01B

2 Using a practice known as Google dorking any number of Internet connected device can quickly be located. http://www.computerworld.com/article/2597539/cybercrime-hacking/feds-issue-bulletin-warning-about-malicious-google-dorking-cyber-actors.html

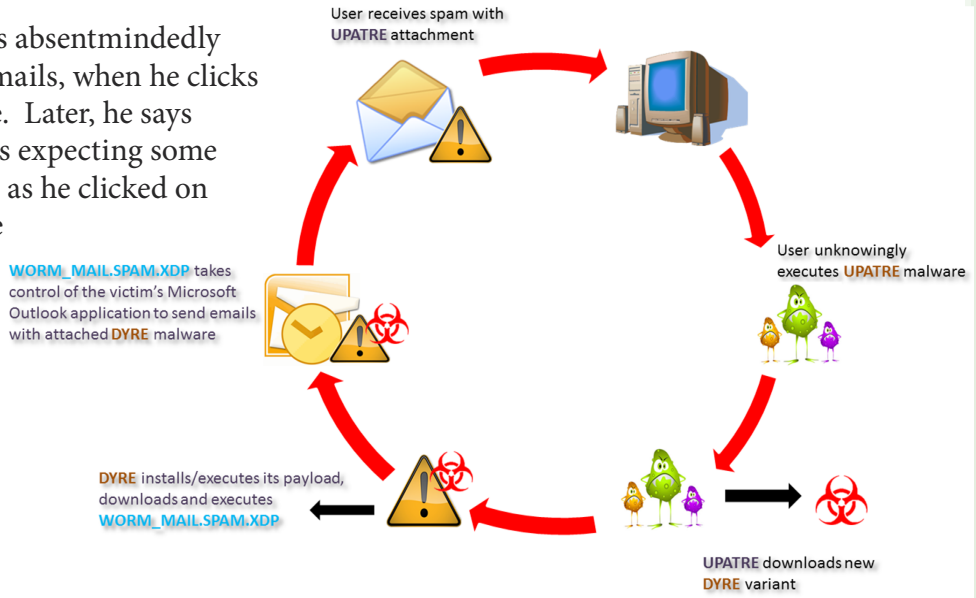
Recently Observed Upatre Malware & Associated Phishing Campaign

Upatre (pronounced: "YOU-pat-ray") is a Trojan horse program commonly delivered through phishing campaigns as a weaponized attachment. Upatre dates back to late 2013 and new variants are generated on a regular basis by malware authors in an attempt to evade detection in an ever-escalating game of cat and mouse with antivirus vendors. Recent versions incorporate a Microsoft Outlook 'hijacker' in an effort to increase the success rate of spam emails by sending Upatre to trusted contacts of the initial victim. This tactic occurred in Florida in a recently observed campaign delivered to thousands of University of Florida email addresses.

Upatre is also a choice platform for hackers and criminals to deliver some virulent malware campaigns involving Cryptowall ransomware, and is especially favored as a vehicle to deliver the Dyreze (Dyre) banking Trojan. Once Upatre infects a computer, the malware sends off for and installs the Dyre malware on PCs in order to steal user IDs and certification information for online banking. Both Upatre and Dyre are updated regularly to avoid detection, and are considered one of the most serious threats to online banking users in the United States. As reported by Symantec, Dyre financial malware is spread through the Cutwail botnet using "short duration, high volume spam attacks targeting millions of users at a time."

Here's how Upatre works:

One day, your brother-in-law is absentmindedly reading through his morning emails, when he clicks on a UPS Ground tracking code. Later, he says it looked totally legit, and he was expecting some packages delivered. But as soon as he clicked on that attachment, **BAM!!!** Upatre is on his PC, and propagating by sending itself out to select recipients from his Microsoft Outlook email list.



Then, immediately after this insidious propagation, Upatre deletes itself.

This malware uses Microsoft Outlook's msmapi32.dll library to log in and send out very realistic looking emails with the misleading attachment. While transmitting, it hides by using the SSL protocol. If it is not able to contact command and control servers, it will instead use URLs it finds through the domain generation algorithm, or connect itself to an I2P address.

As of now, we need to do our best to keep on top of Upatre, so let's keep sending out the word, and keep constant watch for updates.

Trends in Ransomware

Ransomware is a type of malware that restricts a user's access to their computer and files until they pay a ransom. It functions in one of two ways. The first simply locks the system and attempts to socially engineer the user into paying the ransom. Often called the "FBI Virus" or "FBI MoneyPak," typical attempts use threats of criminal prosecution in order to scare users into paying the "fine."

Users receive a notification their system is locked, which cites bogus laws as well as claims of illegal material possession and even images from the local webcam. Needless to say, seeing their own picture on a legal notice supposedly from the FBI, Secret Service, or NSA can scare a number a number of people into acting.

The other ransomware approach is known as *cryptoviral extortion*.[1] The malware encrypts the user's files, making them completely inaccessible. The only way to retrieve the files is to pay for the decryption key and hope the thieves are of a mind to indeed send it to you.

History

The first known ransomware in 1989 (the AIDS Trojan) triggered a payload claiming that the user's license to use a certain piece of software had expired, encrypted file names on the hard drive, and required the user to pay $189 to unlock the system. For the next 20-plus years other ransomware schemes emerged but not in any significant way. That is, until 2013 with the evolution of Cryptolocker and its frequent use of bitcoins as a method of payment.

In this recent iteration, there is no claim of broken laws or contraband materials, and no social engineering. Just a straightforward statement: "Your files are encrypted; if you want to see them again,

Secure FLORIDA.org
Florida Department of Law Enforcement
Florida Fusion Center
Florida Infrastructure Protection Center

LET US KNOW:
(850) 410-7645
Admin@SecureFlorida.org

pay for the decryption key." The price for the key is generally not too outrageous, usually $300-$500.

This is not resolved simply by running your antivirus software. With Cryptolocker, having the key is the *only* way to retrieve your files. In early Cryptolocker versions, it was sometimes possible to read the key off the local computer and retrieve your files. However, in later improvements of the

malware this has been rendered impossible, as the key is stored only on secured servers.

In June 2014, the FBI and a number of other international law enforcement agencies were successful in taking down the GameOver botnet and its associated Cryptolocker ransomware.[2] Alas, the celebrations were short-lived, as soon afterwards all the crypto-clones began to appear, such as CryptoWall and TorrentLocker. While each piece has variations, the functions are identical.

How the infection spreads

Like any other malware, ransomware spreads through human interaction. Unsafe security practices such as downloading files from unknown sources, clicking links on untrusted websites, and responding to phishing emails allows the software to install on your machine.

What if you are infected?

If your computer or network gets hit with encryption ransomware you have two choices: pay the fine and hope for the best, or kiss your files goodbye. (Important note here--a backup can save you. See Protections below.) So what's the answer - Pay or not pay?

Not Pay: For years, security experts have been urging victims not to pay the ransom. First, there is no guarantee that you will actually get the correct encryption key; you may just waste your money. They may even ask for more. Paying the ransom has often been a crapshoot, since you were just as likely to get stiffed. Second, by paying the ransom you incentivize the thieves to continue their practice.

Pay: On the other hand simply writing your files off may not be an option. If your entire business is at stake, a few hundred dollars are probably worth it.

The future of ransomware

The trends suggest that ransomware is not going away any time soon. In fact, the general reluctance to pay the ransom seems to have caused the creators to rethink their business model. There is evidence that the thieves are willing to work with their victims to ensure that both parties are at least somewhat satisfied.[3] Some creators have also become more targeted in their ransom demands, in that the price is based on the data and its value to the owners.

The rise in popularity of near-anonymous bitcoins makes them perfect legal tender for remote criminals, so much so that most attacks include detailed instructions in buying and sending the bitcoins. As with recent identity theft, medical data is likely to feature high in future ransomware attacks.

Another especially frightening ransomware target is the mobile device. Mobile ransomeware is still relatively rare, yet indicatiors suggest the threat is on the rise in countries including the U.S.[4]

Protections

1. Frequently backup your files.

This is the single most important thing you can do to protect yourself from data loss due to

Florida Department of Law Enforcement
Florida Fusion Center
Florida Infrastructure Protection Center

Let Us Know:
(850) 410-7645
Admin@SecureFlorida.org

ransomware. Once you've been infected, the only way to get access to your files back is by paying for the encryption key. And although the bad actors may be more thieves than fraudsters, there's still no guarantee that they will deliver the key once you send the ransom.

When you are backing up your files, it's critical to remember that Cryptolocker and its cousins also infect any mapped drives, such as external hard drives, USB drives, and even network drives if you have mapped them (that is, assigned them a drive letter). So make sure your backups have no connection whatsoever to your computer. And remember to include your mobile devices in your backup efforts.

2. Make sure your backup files can be successfully restored.

Many organizations that invest in a file backup solution fail to test their restore function. When they need it to work, they find that they cannot restore all the files that they backed up, rendering the backup efforts futile. Periodically restore your files and verify the quality and integrity are still intact.

3. Keep your security software up to date.

Your updated antivirus and antispyware will help protect your system from the malicious software that encrypts your files and demands the ransom. Take advantage of security features/addons that work with your browser. Set these to apply updates automatically.

4. Encourage security awareness.

Whether your concern is your company computer or your own home network, the best way to deal with malware is to prevent it from taking hold in the first place. Encourage all users on your network to follow best practices:

- Never click on links in emails from unknown sources
- Never download files from untrusted sites
- Research any files before you install them
- Never release confidential information to unverified individuals

---

1 http://en.wikipedia.org/wiki/Ransomware

2 A botnet is a network of computers infected with malicious software and controlled as a group without the owners' knowledge.

3 http://www.networkworld.com/article/2894507/opensource-subnet/some-cybercriminals-are-improving-customer-service-for-their-victims.html

4 http://www.zdnet.com/article/mobile-malware-on-the-rise-worldwide-ransomeware-hits-the-spotlight/

Florida Department of Law Enforcement
Florida Fusion Center
Florida Infrastructure Protection Center

Let Us Know:
(850) 410-7645
Admin@SecureFlorida.org

Dispatch Highlights

This section highlights articles from past FIPC Dispatches that our analysts think are noteworthy based on trends we're seeing in Florida. The FIPC Dispatch is a list of open-source articles that is sent out twice weekly. If you are interested in receiving *The FIPC Dispatch* **Let Us Know**.

This content is intended as an informative compilation of current/open-source cyber news for the law enforcement, cyber intelligence, and information security communities.

Contents

Forbes Web Site was Compromised by Chinese Cyberespionage Group, Researchers Say

http://www.washingtonpost.com/blogs/the-switch/wp/2015/02/10/forbes-web-site-was-compromised-by-chinese-cyberespionage-group-researchers-say/

- Chinese hackers hijacked Forbes.com and used the site as part of an attack on the U.S. defense and financial industry.
- The hack comes amid growing concerns that even the most trusted sites can be used by hackers aimed at infiltrating sensitive industries.
- The attack worked by leveraging two undisclosed coding flaws — typically called "zero day" vulnerabilities.

Analyst Note: This attack represents the fact that trusted sites are not immune. In fact, this watering hole attack was craftily designed to target a very specific demographic. Vigilance and awareness on the part of end users is difficult to train for such attack vectors. However, healthy suspicion is key to information security.

Malware Presence on Internet Rises by 159% in 2014

http://www.ibtimes.co.uk/malware-presence-internet-rises-by-159-2014-1490626

- There was a 159% increase in malware URLs in 2014.
- The average daily number of emails containing malware increased by 50% to 2.5 billion.
- Cybercriminals are now increasingly targeting smartphone users as well by authoring mobile malware.

Analyst Note: Gone are the days of spectacle malware such as the "I love you" worm. Today's malware largely moves quietly in the background, and so most people who rely on antivirus programs to defend their computers may not know if they are infected. If the computer works and no alarm sounds we believe we are free of malware. This article highlights the fact that malware is increasingly present.

SecureFLORIDA.org
Florida Department of Law Enforcement
Florida Fusion Center
Florida Infrastructure Protection Center

Let Us Know:
(850) 410-7645
Admin@SecureFlorida.org

Kaspersky: 'A Very Bad Incident' Awaits Critical Infrastructure

http://www.networkworld.com/article/2895095/security0/kaspersky-a-very-bad-incident-awaits-critical-infrastructure.html

- Cyber-terrorism attacks against critical infrastructure loom as threats that could become harsh reality.
- Organizations need to discuss risks to critical infrastructure and develop strategies for dealing with them.
- The threat against critical infrastructure is growing.

Analyst Note: As critical infrastructure components heavily rely on Internet connectivity to function, control equipment is increasingly vulnerable to attack. Every day more equipment connects and the potential risk grows. We maintain that awareness needs to increase in the realm of ICS security.

Microsoft Wants to Kill Passwords with Biometric Authentication in Windows 10

http://www.computerworld.com/article/2898654/microsoft-wants-to-kill-passwords-with-biometric-authentication-in-windows-10.html

- Microsoft is out to kill passwords by providing an option to log in to its upcoming Windows 10 OS, applications and Web services via fingerprint, face or iris detection.
- For face and iris recognition, the technology in Windows 10 will initially work on PCs shipping Intel's RealSense 3D camera.
- The authentication relies on infrared technology, which is already built into Intel's RealSense camera.

Analyst Note: We agree. Passwords are dead. Granted, we understand a worthy replacement is still far off. Anything to better authenticate technology raises the bar for information security.

Help us improve *The Secure Florida Beacon.* Please take a moment to complete our survey.

www.surveymonkey.com/s/TheSFBeacon6

Florida Department of Law Enforcement
Florida Fusion Center
Florida Infrastructure Protection Center

LET US KNOW:
(850) 410-7645
Admin@SecureFlorida.org