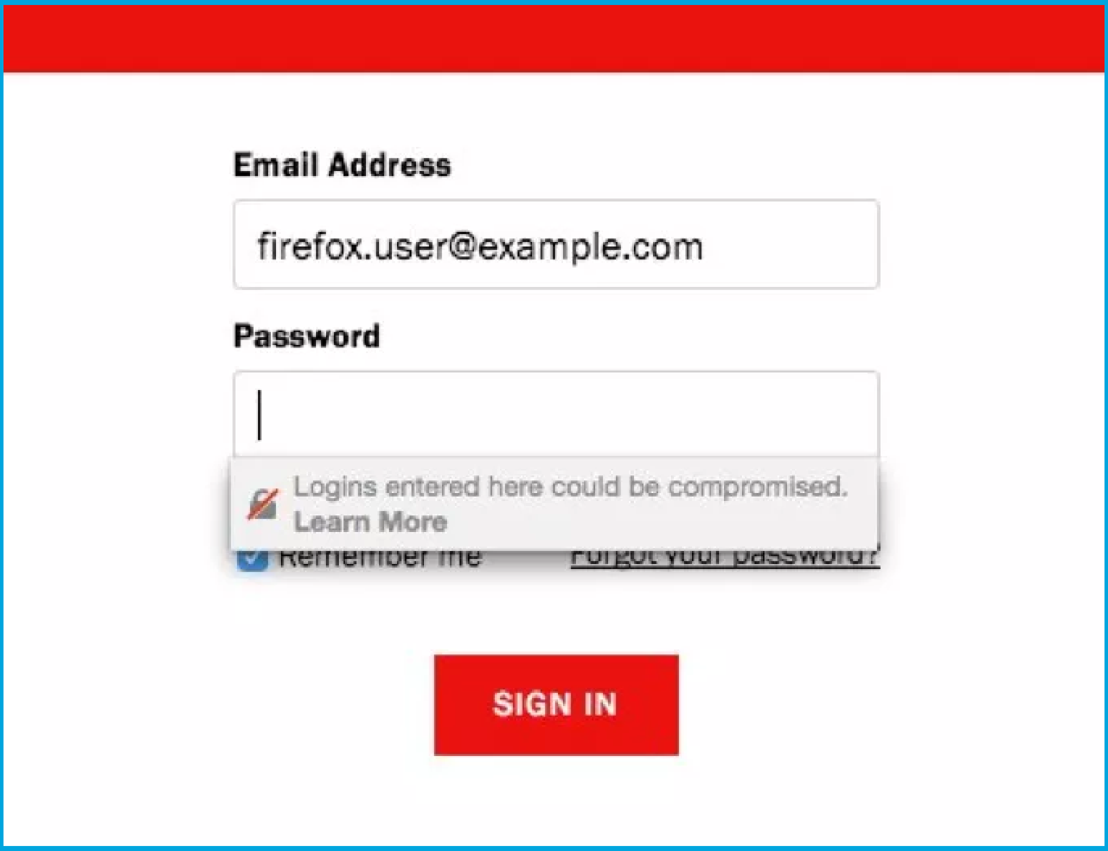
kindred

Security Newsletter

31 March 2017

Firefox gets complaint for labeling unencrypted login page insecure



Email Address

firefox.user@example.com

Password

Logins entered here could be compromised. Learn More

The operator of a website that accepts subscriber logins only over unencrypted HTTP pages has taken to Mozilla's Bugzilla bug-reporting service to complain that the Firefox browser is warning that the page isn't suitable for the transmission of passwords.

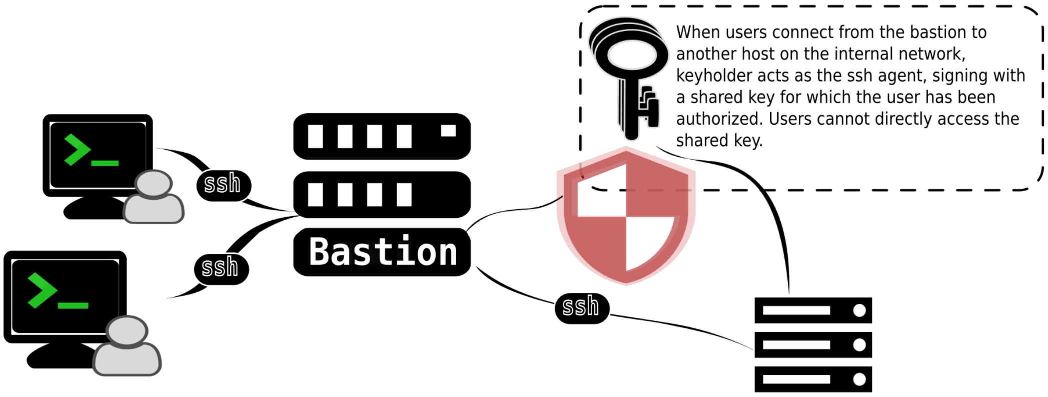
As a member of the Mozilla developer team pointed out in reply to the complaint, both Firefox and Chrome routinely issue warnings whenever users encounter a login page that's not protected by HTTPS encryption. The warnings became standard earlier this year.

When your site requests a user's password over HTTP, the transmission of these passwords is done in the clear. As such, anybody listening on the network would be able to record those passwords. This puts not just users at risk when using your site, but also puts them at risk on any other website that they might share a password with yours.

Needless to say that any website that takes security of their customers seriously should at least enforce https on login pages, if not on the whole website.

Read More

Announcing Keyholder: Secure, shared shell access


ssh
ssh
Bastion
ssh
When users connect from the bastion to another host on the internal network, keyholder acts as the ssh agent, signing with a shared key for which the user has been authorized. Users cannot directly access the shared key.

Keyholder, a newly open-sourced project from the Wikimedia Foundation, is a bit like that ever-watchful security minion. For us, it allows authorized developers to access remote servers using an ssh key, to which it is the only user that has access. More specifically, Keyholder is an ssh-agent proxy that allows a group of trusted users to share an SSH identity without exposing the contents of that identity's private key.

ssh-agent is a program that allows a user to hold unencrypted private keys in memory for use in public key authentication. ssh-agent is neat – it means you only need to enter the password for your private keys once per login session. ssh-agent is also a way you can be bad at public key authentication.

A common use of the ssh-agent is to "forward" your agent to a remote machine. You can then use the socket that that agent creates to access any of your many (now unencrypted) keys, and login to any other machines for which you may have keys in your ssh-agent. So, too, potentially, can all the other folks that have root access to the machine to which you've forwarded your ssh-agent.

Several years ago there were some folks around here who pondered this exact problem and came up with a pretty novel solution that we've finally made into a standalone project!

Read More

eBay to ‘downgrade’ verification by switching to SMS

For a decade, eBay customers who wanted extra-strong security have been able to use two-factor authentication (2FA) involving a Verisign-manufactured key fob. Now, however, eBay’s hardware 2FA option is going away.

KrebsOnSecurity reports that eBay is asking key fob users to start receiving their 2FA security codes via SMS text message instead. Krebs found eBay’s timing ironic: security experts at the US National Institute for Standards and Technology (NIST) recently began actively discouraging the use of SMS-based 2FA in government systems as they are vulnerable to interception… thieves can divert the target’s SMS messages and calls to another device (either by social engineering a customer service person at the phone company, or via more advanced attacks like SS7 hacks).

eBay certainly isn’t the only company that has sought to move away from hardware tokens, which traditionally had a reputation for being costly to provide and manage. If you’ve already got a hardware fob, it still works – for now. And **if you’re not using 2FA at all, eBay’s SMS-based 2FA is still much better than nothing.**

Read More

New IIS 6.0 Zero-Day Exploited in Live Attacks Since July 2016

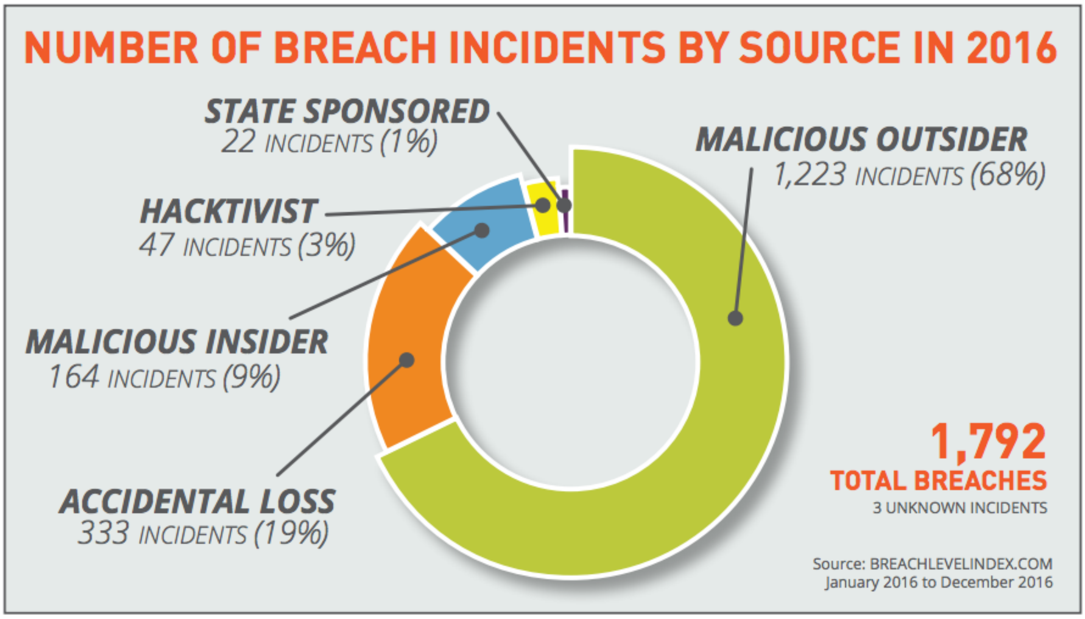
Since July 2016, attackers have been using a zero-day in IIS 6.0 to compromise and take over Windows servers. **Microsoft acknowledged the flaw, but said it couldn't patch it as it affected EOL products, for which it doesn't issue updates anymore.**

The vulnerability only affects IIS 6.0, which was released in November 2010, and shipped with Windows Server 2003 and Windows XP Professional x64 Edition. IIS 6.0 accounts for around 11.3% of all IIS installations, according to data from W3Techs, while IIS overall takes up 11.4% of the entire web server market.

According to the Chinese security experts, the IIS 6.0 zero-day affects the WebDAV service included by default in all IIS distributions. WebDAV is an extension of the HTTP protocol that simplifies sharing and content authoring. **Server owners should update IIS servers to a newer version, unaffected by this issue, or at least disable the WebDAV service if they can't upgrade servers for technical reasons.**

Read More

1.4 Billion Data Records Exposed in 2016 Breaches



Source: BREACHLEVELINDEX.COM
January 2016 to December 2016

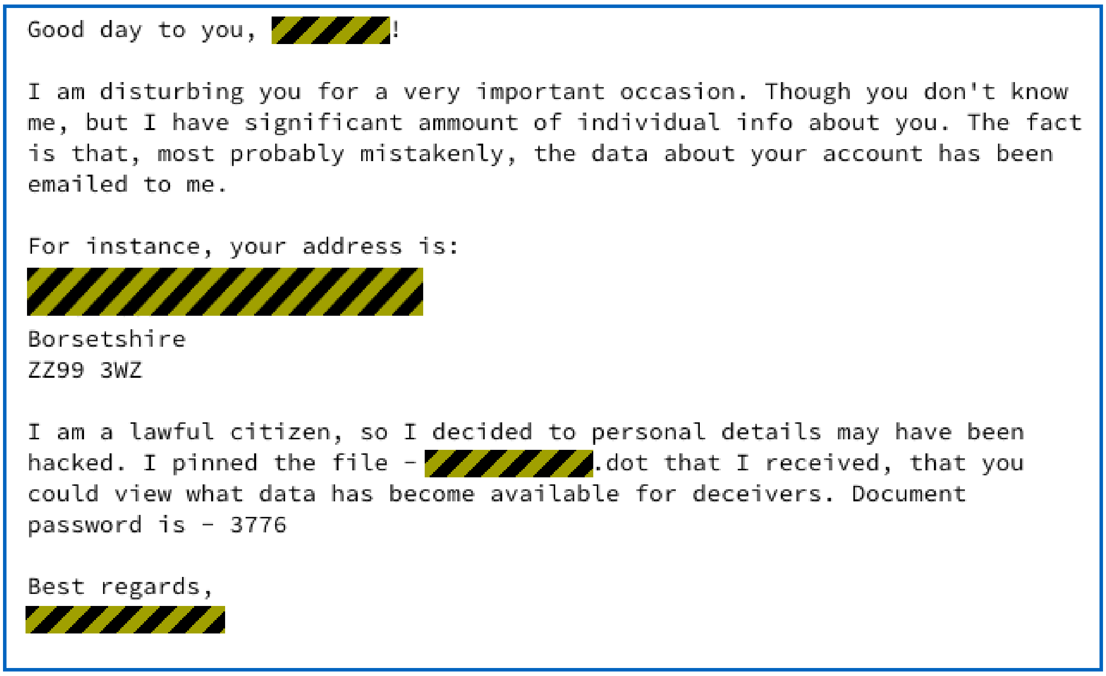
Cybercriminals infiltrated some 1.4 billion data records last year – a whopping 86% increase over the previous year, according to a new report released today by digital security firm Gemalto.

Identity theft accounted for 59% of the data breach incidents, a 5% increase from 2015. Account access-based breaches was next in line as the most prevalent type of data breach. The most targeted industries included technology, which incurred 11% of the breaches. Healthcare was hit with 28% of all data breaches and financial services, 12% of data breaches.

This year only 75 of the data breaches (or 4.2% of the total) involved data that had been encrypted in part or in full. If it's not already the case: **Time to encrypt your sensitive data!**

Read More

The scam that knows your name and home address



Good day to you, [redacted]!

I am disturbing you for a very important occasion. Though you don't know me, but I have significant ammount of individual info about you. The fact is that, most probably mistakenly, the data about your account has been emailed to me.

For instance, your address is:
[redacted]
Borsetshire
ZZ99 3WZ

I am a lawful citizen, so I decided to personal details may have been hacked. I pinned the file - [redacted].dot that I received, that you could view what data has become available for deceivers. Document password is - 3776

Best regards,
[redacted]

Many UK residents woke up recently to a rude internet shock: a scam email that greeted them with their real name and home address. But in this case, the email wasn't trying to disguise that it came from a ne'er-do-well. With so many data breaches in the news recently, it's perfectly reasonably to wonder, "How serious is this?" So it feels wrong and risky not to open it to see how much is in there

To get you to agree to run their malicious macro program, the crooks use what you might call a bait-and-switch trick. The document presents an official-looking help page that tells you that you need to "Enable editing" to view its content. If you click on [Enable Content], you're agreeing to execute a malicious VBA program.

What to do then? Don't open unsolicited or unexpected attachments, especially not on the say-so of an unknown sender. More importantly, don't turn off important security settings such as "macros have been disabled", especially not on the say-so of an unknown sender.

Read More

PicoCTF 2017, a hacking contest and computer security education tool, opens today!

Objective

Investigate your father's room for more clues.

PicoCTF is a computer security game targeted at middle and high school students. The game consists of a series of challenges centered around a unique storyline where participants must reverse engineer, break, hack, decrypt, or do whatever it takes to solve the challenge. **The challenges are all set up with the intent of being hacked, making it an excellent, legal way to get hands-on experience.**

This year's competition features a brand new adventure. When your friend disappears unexpectedly, you must learn and use computer security skills to uncover and decipher critical evidence behind their whereabouts. Can you find your friend before it's too late?

PicoCTF will be on from March 31 to April 14, go subscribe and have fun hacking!

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.