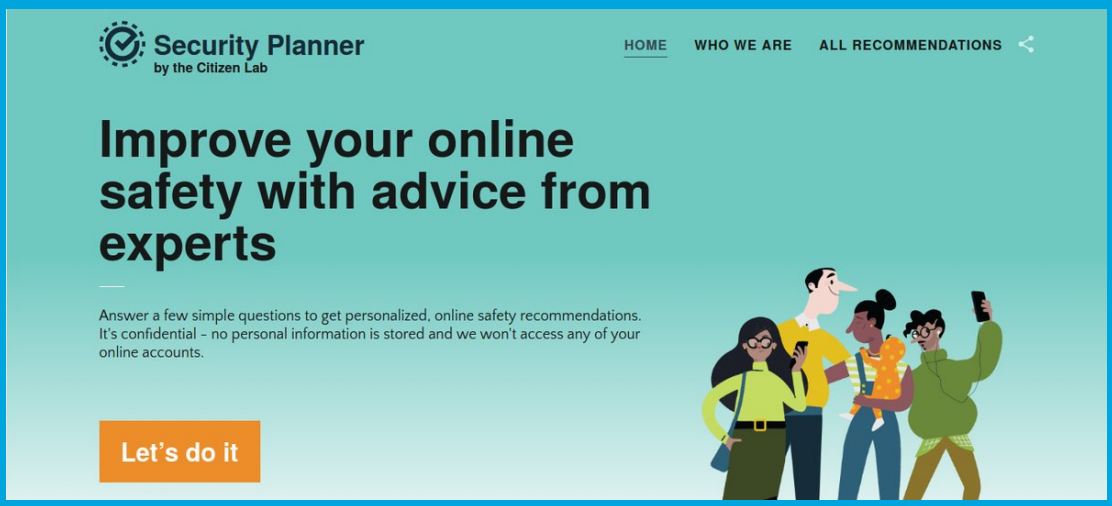
kindred

Security Newsletter

18 December 2017

Subscribe to this newsletter

Security Planner: Improve your online safety with advice from experts



Many of us feel we could be doing more to stay safe online, but it can be hard to decide where to start and which advice to follow. We are often asked about security advice "for the rest of us." Fortunately, experts tend to agree that there are basic steps that anyone can take to make their accounts and devices safer. We believe that these practices work like a vaccine: when more people take steps to be safer, everyone's safety increases.

Security Planner is an easy-to-use platform with tested, peer reviewed recommendations for staying safe online. With just a few clicks, Security Planner tailors straightforward recommendations based on someone's digital habits and the technology they use. Recommendations are presented with clear language, making it easier to decide if they are right for someone. Our goal is to put people in a position to move from learning to action.

Finally, it asks questions to identify people who, because of who they are or what they do, may face additional risks. Since these users are likely to require deeper, more personalized assistance, Security Planner points them to organizations and resources that offer these specialized services.

Our recommendations are developed by a peer review committee of experts from universities, non-profits, and the private sector. This approach ensures that no private company can exercise influence over the products or services that we recommend. Security Planner is also overseen by an advisory board whose members include some of the world's leading thinkers and practitioners in the digital security space.

Clear advice and simple steps for your personal online safety are only a few clicks away. See for yourself at Security Planner.

Security Planner

Original statement

Three Hackers Plead Guilty to Creating IoT-based Mirai DDoS Botnet

The U.S. Justice Department on Tuesday unsealed the guilty pleas of two men first identified in January 2017 by KrebsOnSecurity as the likely co-authors of Mirai, a malware strain that remotely enslaves so-called “Internet of Things” devices such as security cameras, routers, and digital video recorders for use in large scale attacks designed to knock Web sites and entire networks offline (including multiple major attacks against this site).

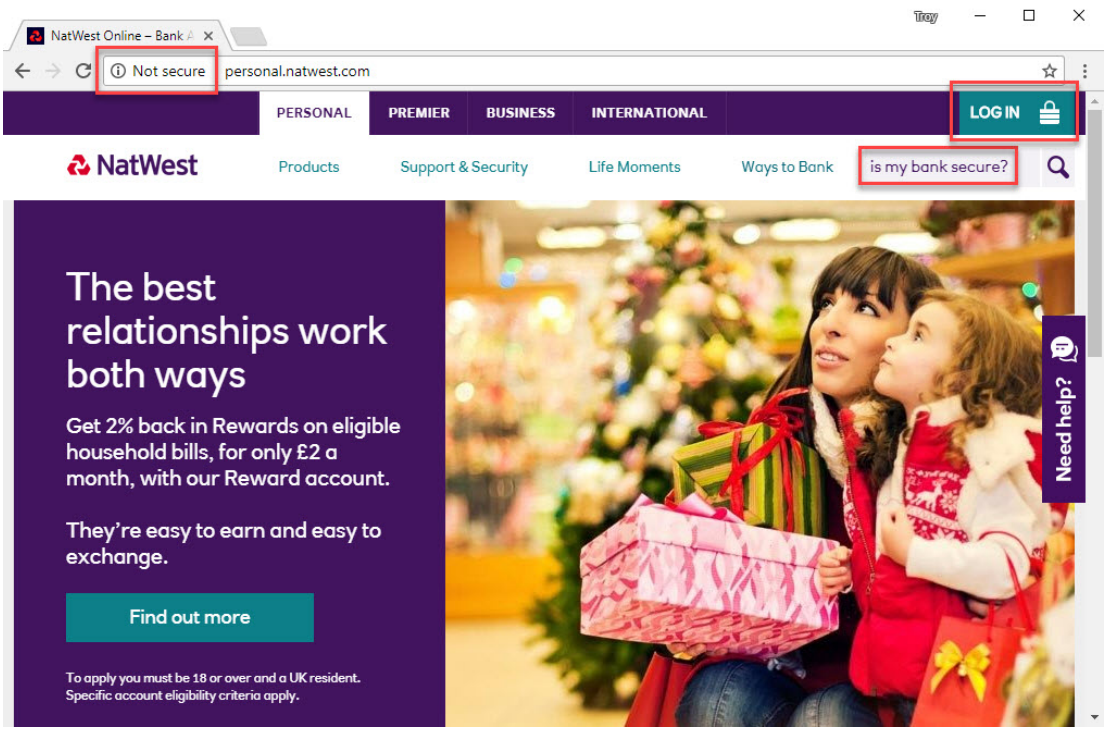
Jha and White were co-founders of Protraf Solutions LLC, a company that specialized in mitigating large-scale DDoS attacks. Like firemen getting paid to put out the fires they started, Jha and White would target organizations with DDoS attacks and then either extort them for money to call off the attacks, or try to sell those companies services they claimed could uniquely help fend off the attacks.

The Mirai malware is responsible for coordinating some of the largest and most disruptive online attacks the Internet has ever witnessed. That September 2016 digital siege maxed out at 620 Gbps, almost twice the size of the next-largest attack that Akamai — Krebs' DDoS mitigation provider at the time — had ever seen.

Read More

Even More

I'm Sorry You Feel This Way NatWest, but HTTPS on Your Landing Page Is Important

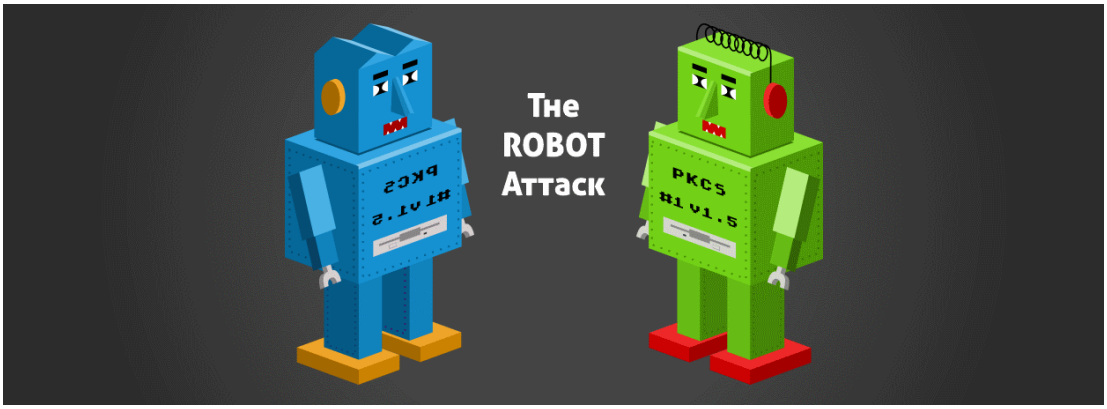


This was after a concerned customer and then myself trying to explain to them that serving their home page over a non-secure connection wasn't such a good idea. The "I'm sorry you feel this way" tweet was in response to me laying things out in what Troy Hunt thought was a pretty crystal-clear fashion. Their original argument - and certainly they're not alone in this misconception - is that because the landing page of the website doesn't have anything sensitive on it then it doesn't require HTTPS.

It's served over HTTP so it's not an encrypted connection and can therefore be intercepted, the traffic read, modified or requests redirect to other locations. We're seeing "Not secure" next to the address bar. Then we have the link to the login page which is the source of much of this controversy. That link takes you off to https://www.nwolb.com/default.aspx which is indeed encrypted. The padlock next to that link is of zero functional value and importantly in the context of this post, is the only padlock on the page because the browser won't give you one due to the non-secure connection!

Read More

'ROBOT Attack' Exposed Facebook With 19-Year-Old Bug



Facebook has paid out a bounty to thank some benevolent hackers who made subtle alterations to an 19-year-old attack to potentially steal user accounts. Whilst the social network has fixed, however, many major websites remain vulnerable, the researchers warned.

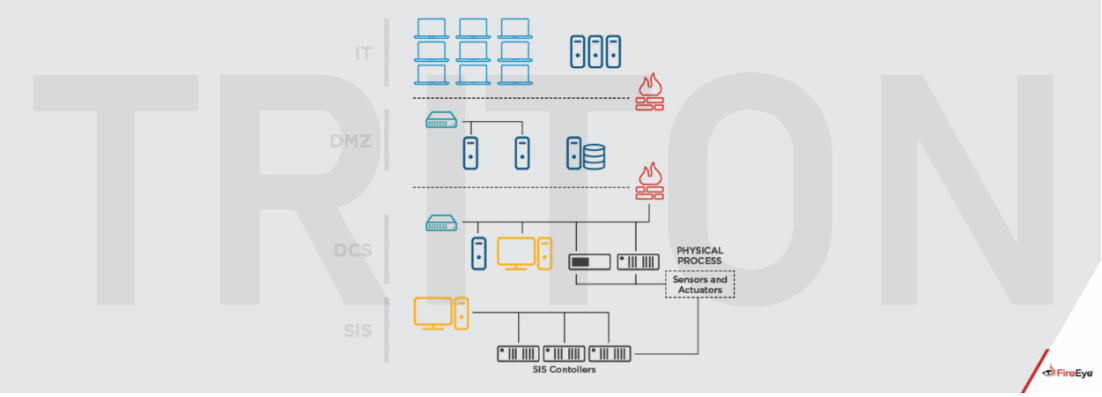
Three security researchers have discovered a variation to an old cryptographic attack that can be exploited to obtain the private encryption key necessary to decrypt sensitive HTTPS traffic under certain conditions. Named ROBOT, which stands for Return Of Bleichenbacher's Oracle Threat, this new attack is a variation of the Bleichenbacher attack on the RSA algorithm discovered almost two decades ago.

Until patches arrive for vulnerable products, the ROBOT research team and US-CERT recommend that owners of vulnerable devices disable TLS session key RSA encryption (also known as RSA encryption mode) on their device. This won't be an issue as most devices also support Elliptic Curve Diffie Hellman (ECDH) session key encryption as a better solution for RSA.

Read More

Even More

TRITON Malware Used in Attacks Against Industrial Safety Equipment



Security researchers from FireEye's Mandiant investigative division have spotted a new form of malware that's capable of targeting industrial equipment.

SIS controllers are special equipment installed in production lines and other industrial setups. They work by reading data from industrial equipment, such as factory machinery, robots, valves, motors, and others. SIS controllers read data streams and make sure the industrial equipment works between certain parameters. If data deviates from a predetermined safety margin, the SIS controller takes a set of actions, which in extreme cases can shut down an entire factory or production line, but will protect human lives and equipment.

The malware hidden inside this fake software would read the configuration files it found on the infected SIS engineering workstation, identify SIS controllers, and attempt to deploy certain payloads. The payloads were configured to either shut down the production process or allow SIS-controlled machinery to work in an unsafe state, most likely to trigger physical damage.

Read More

Even More

Microsoft Azure AD Connect Flaw Elevates Employee Privilege

Microsoft today issued a security advisory to alert users to an improper default configuration in Azure AD Connect, which increases the number of "stealthy admins" on corporate networks and makes businesses more vulnerable to targeted attacks.

Preempt researchers found many employees on their customers' networks had some type of unnecessary administrative privilege, which came from unintentional inclusion in a protected administrative group. Active Directory audit systems often miss "stealthy admins," or admins who have higher domain privileges as a direct result of domain discretionary access control list (DACL) configuration.

Several permissions could give stealthy admins full domain admin privileges. Stealthy admins may be non-administrative users who can add users to security groups, which would enable them to make themselves a domain admin at any point. Another is the ability to replicate a domain, which includes the ability to read password hashes from the domain controller.

When you provision Office 365 in the organization, the first thing you need to do is sync the on-prem directory with the cloud directory," says Ziner. When Azure AD Connect is installed, it creates a service (MSOL) account that syncs directories to read on-prem passwords. This is a "stealthy admin" account: it can access passwords but doesn't have strong security measures.

The company also recommends moving the AD DS account used by Azure AD Connect, and other privileged accounts, into an Organization Unit that is only accessible by highly trusted admins. When giving reset password permissions to specific users, limit their access to only user objects they are supposed to manage.

Read More

The 2018 Guide to Building Secure PHP Software

As the year 2018 approaches, technologists in general—and web developers in particular—must discard many of their old practices and beliefs about developing secure PHP applications. This is especially true for anyone who does not believe such a feat is even possible.

This guide should serve as a complement to the e-book, PHP: The Right Way, with a strong emphasis on security and not general PHP programmer topics (e.g. code style).

Read More

Cutting room floor

- Don't Trust the Host Header for Sending Password Reset Emails
- New (free) Digital Training to Help You Learn About AWS Cloud Security
- Securing communications between Google services with Application Layer Transport Security
- How Google protects your data in transit
- The Good, The Bad and The Ugly of Safari in Client-Side Attacks
- How to Install the Built-In Windows 10 OpenSSH Server
- Patch Tuesday, December 2017 Edition
- AppLocker – Case study – How insecure is it really?
- How to harden Applocker - Block the bypass technique
- Hiding content from Git + more on escape sequences
- Cryptojackers Found on Starbucks WiFi Network, GitHub, Pirate Streaming Sites
- Introducing the New GDPR Center and "Navigating GDPR Compliance on AWS" Whitepaper
- Breaking Out HSTS (and HPKP) on Firefox, IE/Edge and (possibly) Chrome.
- How Our Password Check Works

Tools

- Anubis: Subdomain enumeration and information gathering tool
- RetDec: retargetable machine-code decompiler based on LLVM.
- Makin: Reveal anti-debugging tricks
- Yara Sweeper: Run yara rules in a large scale environment.
- CryptSky: an open source, fully python ransomware PoC.
- https://medium.com/@clong/introducing-detection-lab-61db34bed6ae

This is the last Kindred Security Newsletter for 2017

It's time for the Kindred Group Security team to take some holiday. The newsletter will be off for a few weeks during Christmas and New Year's Eve. But don't worry, we'll be back. See you soon for some awesome infosec news!

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.

You can access the previous newsletters at https://news.infosecgur.us