COMMUNITY INSTITUTION & ASSOCIATIONS RISK SUMMARY REPORT

TLP: Green | CTL: Elevated | PTL: Guarded | Terrorism TL: Elevated | Week of July 10

In This Issue

News and Risk Information

Summary:

Below are some of the top news and risks that the Financial Services Information Sharing Analysis Center (FS-ISAC) has observed this week for community institutions (CI).

NEWS

Cyber-Attack Against Payment Systems Exercise Reminder. If your institution has not signed up to participate in the CAPS exercise (September 12-13), you still have time to register. Participating in the CAPS exercises not only challenges response teams but also helps teams: Discover gaps in incident response plans; strengthen team relationships; build a clearer understanding of system vulnerabilities; and drive exploration of improvements in response processes. To have some of your questions answered, please visit our FAQ page. Registration ends on September 6.

Fall Summit Reminder. The 2017 FS-ISAC Fall Summit at the Baltimore Marriott Waterfront, October 1-4 will be here before you know it – so don't wait to register.

The agenda is comprised presentations by over three dozen senior executive FS-ISAC members, interactive sessions that allow for strategic and solution-oriented discussion; actionable information and sharing designed specifically for financial services institutions; community banks and credit unions; and concrete take-aways including case studies and best practices.

You'll want to be present to hear former CIA Director John Brennan address the general assembly.

RISKS

Intrusion at Nuclear Plants Mark New Cyber Challenges. *Bloomberg* and other news agencies have reported that at least 12 US nuclear facilities have been breached since May by hackers from a foreign government, but the attacks were limited to administrative and business networks, per the Department of Homeland Security and the Federal Bureau of Investigation.

While unsuccessful and apparently not severe enough to trigger public safety alert systems, the malicious actors could be positioning themselves to eventually disrupt the nation's power supply.

Micro Market Vendor Warns of Bankcard and Biometric Data Breach. *Threat Post* writer Tom Spring reports Avanti Markets, which specializes in self-serve food kiosks typically located in company breakrooms, said an undisclosed number of its 1.5 million customers may have had their personal and bankcard data compromised along with stored biometric data. It's unclear what biometric data may have been associated with accounts. However, according to a description of the company's kiosk technology, customers have a "Pay with Fingerprint Scanner" option.

This Week's Top Risks

- **Malware, Ransomware and Trojans**
  - Canada Post Zeus Panda
  - Cobalt Gang
  - LokiBot
  - Pony Malspam
  - Smoke Loader (aka Dofoil and Sharik)
- **System Vulnerabilities**
  - Adobe (multiple), CISCO (multiple), Microsoft (multiple), Struts
- **Themed Phishing Campaigns**
  - Anonymous DDoS
  - Multiple bank themed

The Financial Services Information Sharing and Analysis Center (FS-ISAC) is a non-profit corporation that was established in 1999. FS-ISAC is a member-driven organization whose mission is to help assure the resilience and continuity of the global financial services infrastructure and individual firms against acts that could significantly impact the sector's ability to provide services critical to the orderly function of the global economy. FS-ISAC shares threat and vulnerability information, conducts coordinated contingency planning exercises, manages rapid response communications for both cyber and physical events, conducts education and training programs and fosters collaborations with and among other key sectors and government agencies.

Trickbot Malware Targets English-Speaking Regions

Summary:

TrickBot emerged in August 2016 and launched into a testing and development period in what appears to be a banking Trojan project. This malware is a modular Trojan which appears to have some striking resemblance to the Dyre Trojan, both in its internal make up and the infection methods it uses to reach new endpoints.

IBM Trusteer researchers report rising TrickBot campaigns with configurations targeting banks in various English-speaking geographies. Some of the regions impacted include Australia (31%), UK (25%), Canada (10%) and US (7%) to name the top four countries. TrickBot's operators continue to enhance their focus on business banking, aiming for larger bounties in each attack.

TrickBot has been targeting banks in a growing number of geographies in Q2, and we see the trend continuing as we move into the third quarter of 2017. Widening the scope can mean that TrickBot operators are testing the waters in different regions, hoping to find regions where their attacks would be more successful. As the spread to new locales continues, so does TrickBot's deployment of redirection attacks.

Risk to Community Institutions:

- At this time, TrickBot is reportedly being delivered by spam messages carrying Microsoft Office, file, or PDF files into which Microsoft Office productivity files are embedded. The malware gang has been contracting spam services from the Necurs botnet operators, joining other gangs like Dridex, and the groups that spread the Locky and Jaff ransomware.

Remediation:

Information sharing enables institutions to proactively prevent harm to their institution through:

- Training users to be wary of any unsolicited and urgent email, to report them to appropriate personnel whereby they are investigated and stopped.
- Identifying, reporting, and shutting down pages hosting second stage malware payloads prevents the victim's machine to be fully compromised.
- Taking impacted servers offline prevents stolen information from being sent to the attacker.

Supplemental Material:

- Tracking ID: 931839.

Security Awareness: Reaching Your Customers

Summary:

A false sense of security is the last thing a soldier wants going into a conflict – it could result in a fatal injury. Unfortunately, many financial service customers do just that when begin reading their email. A false sense of security could result in clicking on that link that leads to credential stealing malware, ransomware or worse, destructive malware.

Institutions increasingly offer services to customers through remotely accessible technology, such as the Internet and mobile financial services – especially eBanking. Customer education increases awareness about fraud risk and offers effective techniques your customer/members can use to mitigate the risk persuading them to modify their behavior online.

While it would be great to transfer all your knowledge to them at one time and call it done – institutions must consistently provide education and do so in numerous ways. Remember:

- Training does not need to be fancy or impressive – just effective.
- Training leads to reduced security incidents.
- Saves money and preserves relationships with your clients.

Training Solutions	Commercial	Consumer
Monthly Newsletter	✓	✓
Website Security Page	✓	✓
Downloadable Newsletter	✓	✓
Facility Posters	✓	✓
Statement Stuffers	✓	✓
Email Campaigns	✓	✓
'On-Hold" Messages	✓	✓
Video	✓	✓
Outsourced Packages	✓	✓
Client Tools	✓	✓

Cyber Tip of the Month: Protecting Your Website

Summary:

Members of FS-ISAC have been reporting consistent bank themed phishing campaigns. Some of these emails involved spoofed fraudulent websites that mimic a real financial institution's website. Due to the accessibility of the internet and tools such as PhotoShop, skilled malicious acting groups can perform the needed research and obtain information to create these websites.

To illustrate, a malicious actor visits a legitimate institutions website.

By right-clicking on the site, they can view the webpages source code and copy it.

Once obtained they can paste the information in a web development program and create a fraudulent site.

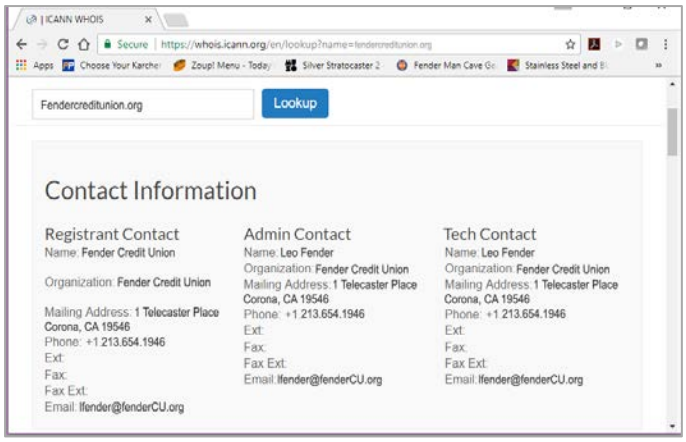
Often, an institution will provide a link for people to review their annual report. The reports provide a wealth of information about the leadership team, corporate assets, locations, etc.

The below WHOIS example was taken partly from two different organizations (the names have been changed to protect the institution).

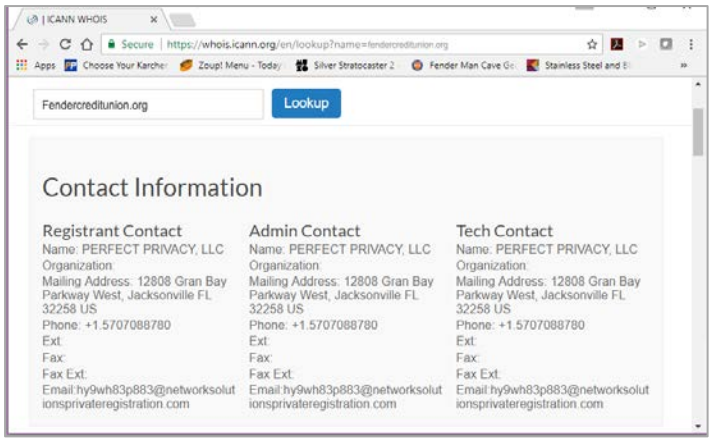
```
<!DOCTYPE html>
<!--[if lt IE 7]>      <html class="no-js lt-ie9 lt-ie8 lt-ie7" lang="en"> <![endif]-->
<!--[if IE 7]>         <html class="no-js lt-ie9 lt-ie8" lang="en"> <![endif]-->
<!--[if IE 8]>         <html class="no-js lt-ie9" lang="en"> <![endif]-->
<!--[if gt IE 8]><!--> <html class="no-js" lang="en"><!--<![endif]--><head>
    <meta charset="utf-8">
    <meta http-equiv="X-UA-Compatible" content="IE=edge,chrome=1">
    <title>Home › [redacted]
    <meta name="description" content="">
    <meta name="keywords" content="">
    <meta name="viewport" content="width=device-width, initial-scale=1, minimum-scale=1, maximum-scale=1">
    <meta name="apple-mobile-web-app-title" content=[redacted]
    <meta name="p:domain_verify" content="8224f95bfad794480e6d1d04af1ef1c6">
    <meta name="google-site-verification" content="tVsjxKqJlUSl_nhg3jF9NDAeoy1RZvZ-M6H6vqsL0Sk">
    <link rel="stylesheet" href="/assets/css/style.css">
    <script src="/assets/js/modernizr-2.6.2.min.js"></script>
    <script type="text/javascript" src="//use.typekit.net/zna0zdk.js"></script>
    <script type="text/javascript">try{Typekit.load();}catch(e){}</script><!-- put in head --><!-- <script type="text/javascript">
    function CheckBoxCheck(type){
        if(type == 0){
            if(document.Q2OnlineLogin.forgot_password[0].checked){
                document.Q2OnlineLogin.forgot_password[1].checked = false;
                document.Q2OnlineLogin.password.disabled = true;
                document.Q2OnlineLogin.password.style.backgroundColor = "#E5E5E5";
            } else {
                document.Q2OnlineLogin.password.disabled = false;
                document.Q2OnlineLogin.password.style.backgroundColor = "#FFFFFF";
            }
        } else if(type == 1){
            if(document.Q2OnlineLogin.forgot_password[1].checked){
                document.Q2OnlineLogin.forgot_password[0].checked = false;
                document.Q2OnlineLogin.password.disabled = true;
                document.Q2OnlineLogin.password.style.backgroundColor = "#E5E5E5";
            } else {
                document.Q2OnlineLogin.password.disabled = false;
                document.Q2OnlineLogin.password.style.backgroundColor = "#FFFFFF";
            }
        }
    }
    </script>
     -->
```

In the first example, the registrant credit union provided contact information for the organizations key players – information that could be used by the malicious actors to initiate additional social engineering and expanded phishing campaigns.

WRONG



RIGHT



Helpful Hints:

It is crucial that institutions take steps to protect information pertaining to their corporate presence on the internet. This can be achieved by using a service that shields your information. In addition, there are other services institutions can use that monitor the registration of variant names of your institution and can identify unauthorized sites and have them taken off-line.

Questions:

If you have any questions about this week's report, please contact Community Institution & Associations. Content provided for internal use by FS-ISAC members. Copyright owners retain all copyrights to material referenced.

Member Services:
admin@fsisac.com
Toll-Free: 877-612-2622 – prompt 1 Outside US: 1 571-252-8517

Security Operations Center:
soc@fsisac.com
Toll-Free: 877-612-2622 – prompt 2