FINANCIAL SERVICES | Information Sharing and Analysis Center

FS-ISAC Monthly Newsletter | February 2018

TLP WHITE

Newsletter Contents

FS-ISAC Response to ATM Jackpotting

FS-ISAC Solutions Showcase – From Intelligence to Action

FS-ISAC AP Summit Call for Presentations Now Open

ISAC Analysis Team Updates

FS-ISAC Annual Summit Registration Open

Upcoming Events and Webinars

*** FS-ISAC members-only**

EclecticIQ Webinar: How to Overcome the Threat Intelligence Cycle Paralysis? | Download until 13 February

Attivo Networks Webinar: Helping Financial Institutions Change the Game on Modern-Day Attackers | 15 February

FS-ISAC Expert Webinar Series: Improving DevOps with Cryptographic Security Practices* | 20 February

Mumbai Member Meeting* | 23 February

FS-ISAC Solutions Showcase* | 28 February

Sydney Member Meeting* | 28 February

London Member Meeting* | 1 March

Zurich Member Meeting* | 7 March

FS-ISAC Expert Webinar Series: How Intelligent Assistants Augment the SOC Team* | 20 March

2018 FS-ISAC Annual Summit
20-23 May | Boca Raton, FL

London Member Meeting* | 14 June

2018 FS-ISAC AP Summit
18-19 July | Singapore

2018 FS-ISAC EMEA Summit
1-3 October | Amsterdam

2018 FS-ISAC Fall Summit
11-14 November | Chicago

FS-ISAC Response to ATM Jackpotting

FS-ISAC distributed several alerts and best practices advisories to assist financial institutions in response to a recent ATM jackpotting vulnerability identified in select locations in the US. In addition, FS-ISAC coordinated with the members of the FS-ISAC's media response team (MRT) to develop and distribute a statement to news organizations covering the ATM jackpotting issue on behalf of the financial services sector. *SC Magazine* and the *American Banking Journal* carried the statement. Starting in Summer of 2017, FS-ISAC acted as a conduit for member-reported activity to law enforcement agencies.

FS-ISAC Solutions Showcase – From Intelligence to Action

Join FS-ISAC on Wednesday 28 February for an all-day members-only event that is uniquely designed to provide members with an exclusive forum to evaluate solutions and ask questions in a low-pressure environment. The theme of this Solutions Showcase is ***From Intelligence to Action***. Join intelligence providers during our morning sessions to see products that help gather threats targeted against the financial sector. Then in the afternoon, providers will demonstrate solutions that focus on making intelligence actionable using their own unique approaches. View the full agenda and register.

FS-ISAC AP Summit Call for Presentations Now Open

FS-ISAC Summits are known for the high-quality, relevant and actionable content presented – and that cannot happen without you! The call for presentations for the 2017 AP Summit (18-19 July, Singapore) is now open! We are seeking proposals for standalone, panel or co-presentations that are educational, content driven sessions that provide actionable, relevant and useful information to attendees. Increase your visibility, share your knowledge and showcase your expertise – submit your proposal for the AP Summit today.

ISAC Analysis Team Update

Dark Caracal

On January 18 the Electronic Frontier Foundation (EFF) and Lookout, a mobile security company, shared their research on "Dark Caracal," an espionage campaign affecting Android mobile devices since 2012. Lebanon's intelligence service, the General Directorate of General Security is the organization held responsible for the campaign. Their targets included journalists and activists, military personnel, manufacturers and financial institutions in more than twenty countries including North America.

Dark Caracal uses tools across mobile and desktop platforms with mobile as their primary attack vector. They purchase or borrow mobile and desktop tools from actors on the dark web to create trojanized Android applications. Lookout discovered Dark Caracal's custom-developed mobile surveillance malware, called

continued, page 2

ISAC Analysis Team Update, continued

Pallas, found in the trojanized Android apps they create. They are also using FinFisher, a tool marketed by Lench IT Solutions, that has been reported to be abused by other nation-state actors. The FinFisher software suite, which the company calls "Remote Monitoring and Deployment Solutions", can take control of target computers and capture encrypted data and communications.

Another malware used by Dark Caracal is a Windows remote access trojan called Bandook RAT. It has a scary list of features that include but are not limited to:

- Firewall bypass method (code injection, API unhook, kernel patch)
- Reverse connection, all traffic through one port
- Rootkit
- PNG/JPEG compressions for screen-capture and webcam
- Remote shell
- Flooding (mailbomb, DDOS attacks)
- Screen manager with screen clicks
- Mic manager (record voice from microphone)
- Keylogger (live)
- Offline keylogger (colored HTML), live passwords, IMs spy with automatic delivery to FTP
- VNC (remote desktop live control)
- Site detection (check all your computers and know which one visits a specific site)
- Screen recorder (record the user activities on the screen into AVI movies)

The *EFF Lookout Report* states that the Dark Caracal infrastructure is likely shared by multiple threat actors and is being used in new campaigns.

Basic steps for protecting yourself from this malware are essentially the same as other phishing attempts. For desktops you should be wary of any emails asking you for sensitive information or tricking you into clicking on a link or opening images and documents that might infect your computer.

For mobile devices

- Keep devices updated and be sure to install patches as soon as they are available.
- Be sure to have a trusted antivirus app installed on all devices.
- Only install apps from verified sources. On Android that means the Google Play Store and on desktop devices like Windows and Macs that means the official app stores.
- Never allow BYOD devices onto corporate networks unless they have been scanned and found clean.
- Personal devices used for work should be controlled under a mobile device management policy.

North Korean Hackers Conduct Six Malware Campaigns

Group 123 also known as TEMP.Reaper is a North Korean group of hackers that have conducted at least six different malware campaigns during 2017 through 2018. Most of the campaigns have been against targets in South Korea. With their latest attack campaign researchers state the hacker group is maturing using a zero-day vulnerability to spread ROKRAT (a remote administration tool) in their latest attacks that represents a first for this group.

The threat group is known to operate on IP addresses assigned to Pyongyang's STAR-KP network, a joint venture between North Korea's Post and Telecommunications Corporation and Loxley Pacific, North Korea's lone ISP. Historically, the majority of their targeting has been focused on the South Korean government, military, and defense industrial base. They have expanded to other international targets in the last year. They have taken interest in subject matter of direct importance to the Democratic People's Republic of Korea (DPRK) such as Korean unification efforts and North Korean defectors based on researcher analysis.

According to researchers, Group123/TEMP.Reaper is distributing the Flash Player exploit (CVE-2018-4878) via malicious Office documents, especially Excel spreadsheets that contain an embedded SWF (Shockwave Flash) file. The exploit downloads a shellcode payload from legit, third-party, South Korean websites that have been compromised. The shellcode, in turn, unpacks and executes a ROKRAT (aka DOGCALL) variant. DOGCALL is a backdoor commonly distributed as an encoded binary file, downloaded and decrypted by shellcode following the exploitation of weaponised documents.

People should be very cautious opening unexpected spreadsheets and document files. You should always be wary of any unexpected or suspicious document. You should also strongly consider uninstalling Adobe Flash. Even if it is disabled in your browser, having it installed on your system is enough for this latest exploit to execute successfully.

While writing this spotlight on Group123/TEMP.Reaper a patch for the Flash Player exploit (CVE-2018-4878) has been released by Adobe, https://helpx.adobe.com/security/products/flash-player/apsb18-03.html. We advise you implement the patch as soon as possible if you use Flash Player | APSB18-03.

Products and Services Discounts

Did you know that as a member of FS-ISAC you can take advantage of special offers and discounts on product and services from our Affiliates and Strategic Partners? **Visit the member discount page** to see current offers. Make sure to bookmark and check back often as offers are updated and added frequently!

FS-ISAC Annual Summit Registration Now Open

FS-ISAC Summits are focused around peer-to-peer networking and building relationships or *circles of trust* with financial services organizations. Registration for the FS-ISAC Annual Summit is now open. Learn more and register today.

Follow us on Twitter @FSISAC or **join the discussion on LinkedIn**.