FINANCIAL SERVICES | Information Sharing and Analysis Center

FS-ISAC Monthly Newsletter October 2016

Newsletter Contents

FS-ISAC Webinars

External Threat Visibility – Looking for Digital Risks Outside the Castle Wall | Easy Solutions | October 11
Register Now

[For International Time Zones]
External Threat Visibility – Looking for Digital Risks Outside the Castle Wall | Easy Solutions | October 11
Register Now

Discovering Your Indicators of Exposure | Skybox Security | October 26
Register Now

Discovering Undiscoverable Threats: Reduce Risk and Enhance Business Defense | BAE Systems | November 1
Register Now

Ready to Replace AV? Criteria to Evaluate NGAV Solutions | Carbon Black | November 3
Register Now

[Case Study] Triage & Collaboration: Improving a Major's Bank Cyber Threat Security Posture | EclecticIQ | November 22
Register Now

Upcoming Events

2016 CAPS Exercises for Financial Institutions in Europe
Europe | October 12 - 13
Register here

2016 CAPS Exercises for Financial Institutions in Asia-Pacific
Asia | October 12 - 13
Register here

Admiral James Stavridis to Keynote Fall Summit

FS-ISAC is pleased to announce an update to our keynote speaker at the 2016 Fall Summit in Nashville. Admiral James Stavridis will address "Sailing the Cyber Sea: The New Realities of 21st Century Security." Admiral Stavridis served as the 16th Supreme Allied Commander of NATO and was the longest-serving combatant commander in recent US history. Admiral Stavridis has published six books on leadership, Latin America, ship handling, and innovation, as well as hundreds of articles, including a monthly column for *TIME Magazine*.

Still Time to Register for the European Summit

Haven't registered for the European Summit in Barcelona yet? No need to fret, registration remains open for the Summit. Here are two of more than 30 informative sessions being offered:

- **Corporate Communication During a Cyber Crisis |** How to plan, execute and assess an international exercise focusing on corporate communications during a cyber-attack. Join us to watch and evaluate how communication departments and communication managers react when a major cyber-attack occurs
- **Going Beyond Malware: Hand to Hand Combat With a Targeted Attacker |** Most breaches are not malware based. This presentation will disclose hard-hitting new facts and insights into recent global attacks and advanced cybercrime targeting large financial services organizations. Based on actual case studies, we will provide important lessons about the attackers' tactics, tradecraft and objectives. Join your peers to learn more about hacker tradecraft and how unified next generation AV and endpoint detection and response, combined with managed threat hunting, provides continuous breach prevention.

Head over to the European Summit page on the website to view the Summit Brochure, agenda and hotel and travel information.

Call for Presentations: 2017 Annual and APAC Summits

FS-ISAC Summits could not happen without our amazing members. Each Summit we turn to them to produce stimulating and creative presentations so that FS-ISAC may produce conferences that you want to attend. Now is your opportunity to provide input for the 2017 APAC Summit in Singapore, April 2-5, and the 2017 Annual Summit in Orlando, April 30-May 3. Please submit your ideas for the APAC Summit between now and October 28, and for the Annual Summit between October 14 and November 30. A member committee will evaluate the proposals and the FS-ISAC will announce the sessions several months before the summit meeting. Make sure to submit your proposal today for consideration. For presentation rules and tips for selection, visit fsisac-summit.com.

Ransomware Roadshow a Big Success

FS-ISAC teamed up with the National Health ISAC, Multi-State ISAC, Palo Alto Networks, Symantec, the FBI, and US Secret Service to conduct 14 Ransomware 101 events across the United States. Dubbed the "Ransomware Roadshow," the first 12 events saw more than 2,600 attendees. If you have not been able to attend an event, there will be two more events held this October, in Chicago on Oct. 12 and in New York on Oct. 20. Be sure to register today!

CAPS North America Recap

The North American Cyber-attacks Against Payment Systems (CAPS) Exercise was conducted the week of September 19 and offered again the week of September 26. CAPS is a two-day exercise and financial institutions could choose either week to participate. Close to 1,700 FIs participated in this year's exercise. That represents an increase of over 700 participants compared to last year's exercise.

Membership Guide Update

An updated version of the membership guide is now available on the FS-ISAC Portal for both U.S. and International members. The new version incorporates an updated list of councils and working groups, enhanced portal alert customization, and a new contacts section. The guides can be found in the portal's document library under "Member Resources."

Upcoming Events (cont)

2016 CAPS Exercises for Financial Institutions in Europe
Europe | October 18 - 19
Register here

2016 FS-ISAC Fall Summit
Gaylord Opryland | Nashville, TN | October 23 - 26
Register here

Member Meeting
Singapore, Asia | October 25
Register here

2016 FS-ISAC European Summit
Crowne Plaza Barcelona Fira Center | Barcelona, Spain | November 6 - 9
Register here

RSA Workshop
Abu Dhabi, United Arab Emirates | November 14
Register here

Member Meeting
Melbourne, Australia | November 17
Register here

Member Meeting
London, United Kingdom | December 6
Register here

Update from the FS-ISAC Analysis Team

Bayrob/Nivdort Malware
Since early September 2016, the FS-ISAC IAT has been receiving reports of phishing emails delivering the variants of the Bayrob (aka Nivdort) trojan. The malware is typically delivered via a phishing email with a .zip attachment, containing a .exe payload file. Recently-observed phishing samples have included Spanish- and Arabic-language emails.

Once the malware is deployed, it creates multiple files and a registry entry that enables it to run every time Windows starts. The malware registers one of the created files as a service with characteristics of a Windows Update service. The service provides a message at startup instructing machine users to keep the service running or their computer may become vulnerable to security issues. This ensures the created service remains running and the malware can carry out its objectives. In addition, Bayrob modifies registry entries to lower internet security settings.

Another characteristic of Bayrob or Nivdort is the modification of the Windows Hosts file to redirect specified URLs to different IP addresses, possibly to prevent it from accessing websites with certain security applications or redirect users to malicious sites.

The malware uses the proxy to connect to a remote host in order to receive instructions, upload information stolen from the victim machine, download and run files, or carry out other malicious objectives.

Remcos RAT
Starting in September, the FS-ISAC IAT became aware of what appears to be a new Remote Access Trojan (RAT), named Remcos.

An Italian malware developer by the name of Viotto or z3r0 has published his latest project, the Remcos RAT which he's selling on underground hacking forums for a price that varies from $58 to $389 – all payable in anonymous digital currency.

The author states that Remcos includes a keylogger capable of both online or offline captures, password dumper integrated with IE, Firefox, Chrome, Safari, Opera, Pidgin, Trillian, Miranda & ICQ, screenshot capabilities and more. The free version is available with limited features, but the pro version includes access to all features.

Symantec also analyzed the RAT and identifies it as Remvio. Their researchers determined the password dumper is effective against Digsby, Paltalk and Windows MSN or Live messenger, but not Safari as Viotto originally claimed.

Remcos only targets Windows PCs - XP and higher for both 32 bit and 64 bit platforms. All data stolen from infected devices is sent encrypted via HTTPS to the command and control server.

Remcos is dangerous due to its ability to queue operations for the RAT to carry out and execute in desired order when the victim comes online. Remcos also has anti-analysis techniques cooked into the code. The RAT will shut down and delete itself if executed in virtual machine environments.