ThreatScape Media Highlights Update – Week Of February 17th

The following is this week's sample of ThreatScape® Media Highlights – an email roundup of security headlines augmented by insights and analysis from iSIGHT Partners. Our cyber threat intelligence clients receive this update daily.

Wednesday, 17 February 2016

Download PDF Version Here

Russian Police Prevented Massive Banking Sector Cyber Attack

From The Media
The Russian Interior Ministry's department of cyber crimes exposed a group that had planned several major cyber attacks on international payment systems and Russian banking systems. According to the department, the group was comprised of over 50 highly capable members with initial plans to steal up to 1.5 billion RUB.
Read the Story: SC Magazine

iSIGHT Partners Analyst Comment
Due to vague media reporting on this subject, it remains unclear whether the activity reported is related to Corkow or GCMAN. Reports appeared to imply that the group disrupted by the Russian Interior Ministry pertained to Corkow, but, given the apparent strong relation between this report and activity recently reported by Kaspersky, we suggest the activity is more consistent with what Kaspersky described as GCMAN activity, which was neutralized before financial institutions experienced significant losses.

Related iSIGHT Partners Reports
ThreatScape Media Highlights ('Covert' APT Attacks Pose New Worries), 10 Feb. 2016
ThreatScape Media Highlights (Russian Hackers Moved Ruble Rate With Malware), 9 Feb. 2016
Intel-1114421 (The Increasing Confluence of Cyber Crime and Cyber Espionage), 20 March 2014

Malware Targets All Android Phones—Except Those in Russia

From the Media

According to CSIS Security Group, a malware strain is targeting all Android devices except for those in Russia. The malware, dubbed MazarBOT, possesses the ability to take full control of a target device and, according to CSIS, appears to be focusing targeting on online banking customers. MazarBOT performs a location test upon installation and will stop if it detects that the device is within Russia.
Read the Story: CSO Online

iSIGHT Partners Analyst Comment
It is typical of Russian-origin malware to disable itself if it detects it is being run on a Russian device, usually because laws in Russia prohibit cyber crime activities targeting the Commonwealth of Independent States (CIS). Also of note, there is a malware family tracked as “Mazar,” “GMBot,” “Slempo”, or “Slembunk” that we judge to be distinct from MazarBOT. While the malware types share a few common functionalities (mainly related to SMS use), the majority of functions and a large portion of the code are different. For example, MazarBOT uses Tor for hiding communication; GMBot does not.

Related iSIGHT Partners Reports
16-00000406 (Continued Market Maturation of the Mobile Threat Landscape: Proliferation of Android Credential Theft Malware), 20 Jan. 2016
15-00012490 (Financial Services Targeted by ‘Mazar’ Android Malware Expands in Europe and Asia-Pacific Regions), 23 Nov. 2015

Critical GLIBC Vulnerability Puts Nearly All Linux Machines at Risk

From The Media

The Linux GNU C Library (glibc) is vulnerable to a critical flaw affecting almost all Linux machines. Glibc was last affected by the Ghost vulnerability in January 2015. The current flaw (CVE-2015-7547) is a stack-based buffer overflow in the glibc DNS client-side resolver. The vulnerability could result in remote code execution.
Read the Story: Threat Post

iSIGHT Partners Analyst Comment
Although a large number of Linux systems are reportedly vulnerable, we consider CVE-2015-7547 to be a medium-risk vulnerability due to the potential for arbitrary code execution, offset by the address space layout randomization (ASLR) bypass requirement. Further, exploitation is easily mitigated by limiting DNS response sizes and verifying DNS queries. Proof-of-

concept (PoC) code is publicly available, but is only capable of causing a denial-of-service (DoS) condition; full exploit code is privately held by Google. We are unaware of exploitation in the wild.

Related iSIGHT Partners Reports
16-00002126 (GNU Vulnerability CVE-2015-7547), 16 Feb. 2016
15-34447 (GNU "Ghost" Vulnerability CVE-2015-0235), 19 Nov. 2015

Espionage Actors Linked to Sony Breach Also Tied to Ongoing North Korean Operations

From The Media
Researchers from Kaspersky Labs and AlienVault have reported that technical indicators from campaigns affecting Samsung and a South Korean nuclear power plant operator demonstrate links to the high-profile breach of Sony in late 2014. These findings indicate that the actors responsible for the Sony hack most likely also have connections to multiple malware families and campaigns including DarkSeoul, TEMP.Hermit and WildPositron—groups and tools believed to be linked to North Korean actors. The newly released information suggests the actors behind the Sony breach (dubbed "The Interviewers") remain at large and are involved in ongoing cyber espionage operations.
Read the Story: SC Magazine

iSIGHT Partners Analyst Comment
Although specific technical indicators have not yet been released (and the researchers have indicated they do not intend to reveal all of their findings publicly), the findings are consistent with previous iSIGHT Partners reporting. Published analysis of Volgmer malware and TEMP.Hermit operations indicates potential connections with other probable North Korean activity. Shared code and a distinct password shared across multiple droppers support the notion that the actors behind the Sony hack are linked to continuing North Korea-nexus campaigns.

Related iSIGHT Partners Reports
15-00011382 (Hangul Zero-Day Leveraged Against South Korean Industry and Government; Volgmer Malware Illuminated as Suspected North Korean Backdoor), 15 Oct. 2015
15-00012308 (TEMP.Hermit Actors Target South Korean Atomic Energy Research Institute), 6 Nov. 2015

China and Russia Step Up Cyber Attacks on Australia

From The Media

Actors are increasingly targeting the Australian Government's secure communications network. Chinese and Russian actors' increased attacks have forced Australian Government agencies to use the Intra Government Communications Network (ICON). Hundreds of attempts are made each month to access the government's ICON system, with China-sourced attacks being the most predominant.

Read the Story: News.com.au

iSIGHT Partners Analyst Comment

We cannot verify a spike in intrusion activity against the Australian Government's secure network. However, the government's initiative to improve cyber defenses suggests that associated bureaus have been compromised or experienced a high volume of intrusion activity. iSIGHT Partners has previously reported on Chinese-nexus activity targeting Australian interests, including 338 Team, UPS Team, Mana Team, and JJDoor malware activity. Further, Russian operators known as Koala Team also targeted Australia as part of a widespread, global campaign to collect proprietary data.

Related iSIGHT Partners Reports

15-00010120 (Activity Connected to JJDoor Targets Australia), 23 Sept. 2015
Intel-1052649 (Koala Team Targeting), 21 May 2014
Intel-940662 (338 Team Activity), 20 Sept. 2013

Russian Cyberspy Group Uses Simple yet Effective Linux Trojan

From the Media

Pawn Storm, a Russian cyber espionage group, is infecting Linux systems with the Fysbis Trojan. The Fysbis Trojan does not require root privilege access, and is also modular, allowing actors to integrate plug-ins for expanded functionality. Fysbis' primary purpose is to steal data, such as documents and web browsing activity.

Read the Story: CSO Online

iSIGHT Partners Analyst Comment

This article refers to malware iSIGHT Partners previously reported as "XAgent," a tool developed and commonly employed by Russian-nexus actors tracked as Tsar Team (aka APT28). The XAgent framework exploits several platforms, including Windows, Linux, and Apple IOS, and is typically delivered through a Sofacy dropper, commonly linked to Tsar Team operations. XAgent has various modules that enable espionage operations, including one that allows propagation in air-gapped networks.

Related iSIGHT Reports
15-00000338 (Tsar Team Overview), 4 Feb. 2015
14-32556 (IOS Malware Being Developed by Tsar Team), 5 Feb. 2015
14-00000063 (Analysis of XAgent Malware Framework), 5 Dec. 2014

The post ThreatScape Media Highlights Update – Week Of February 17th appeared first on iSIGHT Partners.

Source: /ht71-yraurbef-fo-keew-etadpu-sthgilhgih-aidem-epacstaerht/20/6102/moc.srentrapthgisi.www