ThreatScape Media Highlights Update – Week Of February 10th

By Patrick McBride

February 10, 2016

iSIGHT Partners

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, 10 February 2016

Download PDF Version Here

Poseidon APT Group Identified As First Portuguese-Speaking Campaign

From The Media
Kaspersky Lab researchers have been tracking a group carrying out covert attacks on organizations worldwide. The researchers believe they have enough evidence to suggest this is the first ever Portuguese-language cyber espionage group. The Poseidon Group, as it has been dubbed, which has now been active over ten years, lures victims with infected Microsoft Office documents to collect business-sensitive information. The group has targeted businesses in a wide range of countries, even though the language strings in its code and commands are designed to function on Portuguese- and English-language systems.
Read the Story: Threat Post

iSIGHT Partners Analyst Comment
iSIGHT Partners identified and reported activity related to this group in February 2015. The activity we observed focused primarily on Spanish speaking countries, but the information released by Kaspersky gives a deeper understanding of this group and the scope of their operations. The target set Kaspersky listed is consistent with the behavior identified in our 2015 report, and the public report showcases the proliferation of capabilities to an increasing number of actors and the threat these actors can pose to businesses.

Related iSIGHT Partners Reports
15-00000288 (Unknown Cyber Espionage Campaign Targeting Spanish-Speaking Region; Interest in U.S. and UK Governments), 3 Feb. 2015
Intel-1114792 (Country Threat Profile: Brazil), 20 May 2014

Skype Attacked by New Trojan: The T9000

From the Media
Palo Alto Networks researchers have identified a Trojan, dubbed T9000, targeting Skype users. According to the researchers, T9000 is an updated version of the T5000 Trojan.

T9000 is designed to steal victims' data and is capable of taking screen shots and recording audio calls. Furthermore, the Trojan possesses a multi-stage installation process that looks for security software installed on the target machine in order to avoid detection.
Read the Story: IT Pro Portal

iSIGHT Partners Analyst Comment
iSIGHT Partners has observed the T9000 Trojan being used by Chinese espionage actors alongside IEChecker malware to target Tibetan entities. While such activity is consistent with Chinese operators, we do not uniquely associate it to any currently tracked team. The T9000 Trojan is notable for its extensive anti-virus detection and evasion capabilities, which, though not unique to the T9000, are emblematic of the arms race between defensive and offensive cyber operators and demonstrate the need for a multi-layered defense.

Related iSIGHT Partners Reports
16-00000060 (TEMP.Hex Targets US and Chinese Border Nations; Commercial Sector Affected), 11 Jan. 2016
15-00011990 (Chinese Espionage Targets Dissident Media Organizations Using WMIGhost), 29 Oct. 2016
14-00000090 (Country Threat Profile: China), 24 Dec. 2014

Flaws in Trane Thermostats Expose Networks to Attacks

From The Media
Cisco researchers have uncovered vulnerabilities in a group of Trane smart thermostats. According to Cisco's report on the issue, Trane took almost two years to address vulnerabilities in the ComfortLink II thermostat. The most recent of the patched vulnerabilities (CVE-2015-2867) allows an attacker to log into the thermostat over SSH and obtain complete control of the system. Attackers could perform malicious activities such as network reconnaissance using this vulnerability.
Read the Story: Security Week

iSIGHT Partners Analyst Comment
Vulnerabilities affecting Internet of things (IoT) devices present a potential avenue for actors to gain footholds into targeted networks. However, both apparent low actor interest in targeting such devices and limited exploit development suggest that actors are still mainly focused on more traditional targets, such as workstations and mobile devices. Despite this, there are significant long-term security concerns that will need to be addressed in devices such as smart thermostats, as we expect increased interest in targeting such devices in the coming years.

Related iSIGHT Partners Reports
15-00001826 (Open Interconnect Consortium Establishes New Liaisons to Advance IoT Interoperability Standards), 23 March 2015
Intel-1234296 ('Internet of Things' (IoT): Excitement Continues, but Security Concerns

Growing), 15 Sept. 2014

'Covert' APT Attacks Pose New Worries

From The Media
An evolved version of Carbanak, a well-known type of banking malware, is now being used for advanced persistent attacks against companies, including those in the financial sector. The latest version, which Kaspersky calls Carbanak 2.0, has only been observed targeting victims in Russia with the APT-style attacks, leveraging customized malware and covert reconnaissance techniques.
Read the Story: Bank Info Security

iSIGHT Partners Analyst Comment
Carbanak operators' renewed targeting after a significant four-month reduction in activity is marked by a shift to leveraging access to internal financial institution processes in their campaigns. While this financial fraud activity is significant, particularly with its focus on targeting Russian and Ukrainian victims, APT-style activity (or persistent targeted intrusion activity) is not novel for cyber crime as a whole. These attacks, targeting back-end banking systems and other areas of financial institutions' networks, are much less common than financial account takeover or other widespread cyber crime campaigns impacting financial institutions, but they can be much more damaging.

Related iSIGHT Partners Reports
15-00010002 (Carbanak: Malware Behavior, Capabilities and Communications), 23 Sept. 2015
15-00013604 (Cyber Criminal Targeted Intrusions as a Threat to Financial Institutions), 30 Dec. 2015
15-00000558 (Operators Behind 'Anunak' (aka 'Carbanak') Malware Steal Large Amount from Eastern European Financials; Link to Carberp Operators Unsubstantiated), 19 Feb. 2014

Half of Surveyed Canadian Firms Experienced Cyber Attacks

From The Media
A recent study surveying 654 Canadian IT and IT security professionals found that the

number of reported attacks went up by 17 percent in 2015. Furthermore, respondents indicated their organizations faced an average of 40 cyber attacks per year. Fifty-one percent of those surveyed indicated that their organization experienced an attack within the last year that resulted in the loss or exposure of information. Seventy percent of the respondents noted that malware and exploits were able to dodge their intrusion detection systems.
Read the Story: IT World Canada

iSIGHT Partners Analyst Comment
The survey's findings reflect the continued threat malicious adversaries pose to Canadian enterprises. We regularly see adversaries targeting Western European and North American organizations for a variety of malicious activity, likely due to the perceived wealth of organizations and individuals in those regions, and we are certain many organizations are unable to repel all of these attacks.

Related iSIGHT Partners Reports
16-00000604 (Prominent Compromised Database Vendors in the Russian-Speaking eCrime Underground), 26 Jan. 2016
15-00013604 (Cyber Criminal Targeted Intrusions as a Threat to Financial Institutions), 30 Dec. 2015
15-00013110 (Compromised Digital Signature Used to Sign Cmeshell Malware Leveraged Against ASEAN Targets), 25 Nov. 2015

Want to learn more?

Request a Consultation >

Interested in a FREE Trial? >

Download a Datasheet >

Recent Posts

- ThreatScape Media Highlights Update – Week Of February 10th
- ThreatScape Media Highlights Update – Week Of January 28th

- FireEye Acquires iSIGHT Partners

Jay Leek

Chief Information Security Officer, Blackstone

> Blackstone has relied on iSIGHT Partners for the past year to understand and interpret our cyber threat environment. Their products allow us to prioritize resources to counter those cyber threats that pose the greatest risk to our organization. We believe their approach to providing intelligence led security will be the model for the future.

Comprehensive cyber intelligence connecting security technology and operations to the business.
+1-214-731-4585 info@isightpartners.com