AUGUST, 2018
EDITION 19

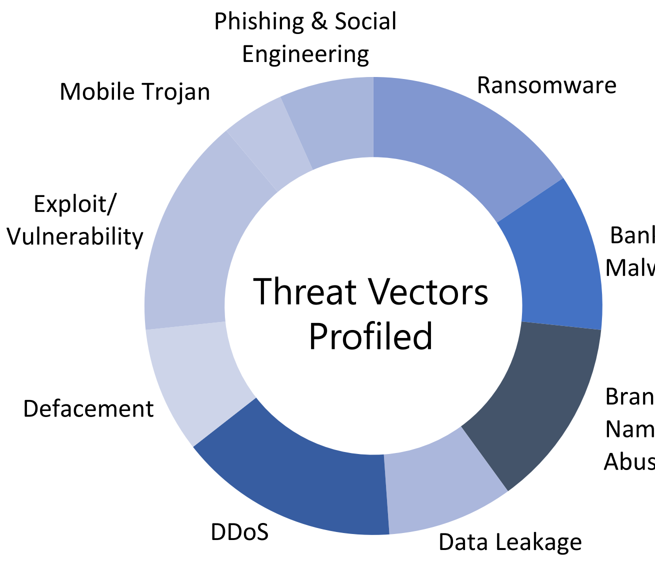
THE MONTHLY CYBER THREAT INSIDER

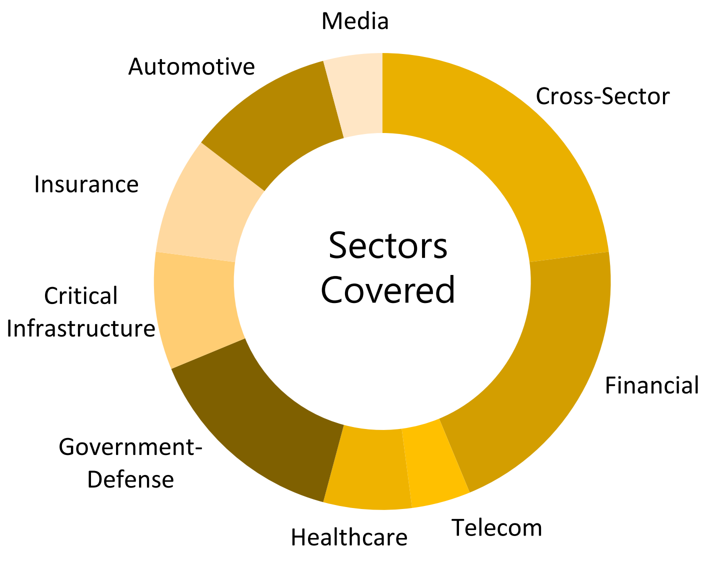
SenseCy A VERINT Company

POWERED BY WEBINT7

TARGETED THREAT INTELLIGENCE: MONTHLY OVERVIEW

SenseCy uses a unique methodology to source a multitude of web-platforms, including deep web forums, darknet marketplaces, closed social media groups, mobile apps and more, producing actionable intelligence alerts and expert reports for its customers. Here is a breakdown of the sectors covered and the threat vectors profiled in the past 30 days:





Source: Dark Web forums, OSINT

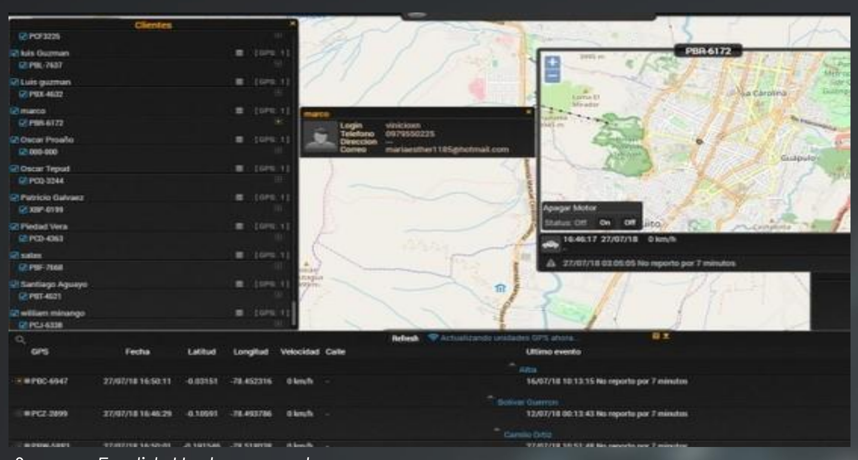
SOURCE CODE OF RATOPAK/PEGASUS SPYWARE RECENTLY LEAKED

On July 6, 2018, a post claiming to contain the source code of Carbanak group malware was published on an underground forum. Soon after the sharing of the code, it was uploaded by an unknown threat actor to the Pastebin platform, making it accessible to all. Researchers who analyzed the shared code discovered the malware is not one used by the Carbanak group, but the Ratopak/Pegasus spyware, used in attacks against Russian banks in 2016.

According to the media, the leaked code was published on an English-speaking forum on July 7, 2018, by a user named FR3D. However, using our sources, SenseCy analysts managed to detect an earlier publication of the code on a Russian-speaking underground forum by a threat actor named Bobby.Axelrod on July 6, 2018. This user appears to be the original source of the leak, as he only posted twice – once, sharing the links for downloading the materials, and another post, titled "PIR Bank Lost 58 million Rubles in a Cyber-Attack," referring to an attack in early July 2018, attributed to the MoneyTaker group that operates against banks in the US, the UK, and Russia. Based on these two posts, we assume this threat actor links between the leak and the attack, claiming the leaked malware was used in this recent attack and attributing it to the MoneyTaker attack group.

The publication received numerous replies by the forum members, mostly writing about the sensitivity of the materials, and speculating they were most likely provided by insiders familiar with the Russian banking system. Since attacks against Russian banks are not welcomed on Russian underground forums, we witnessed very restrained replies on the publication. However, we believe that numerous threat actors will use the malware in future attacks, after modifying and upgrading it.

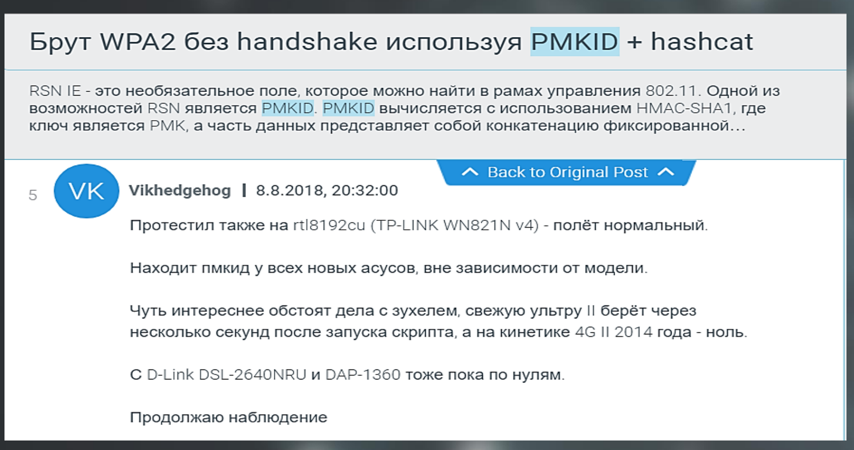
READ MORE ON OUR BLOG



Source: English Underground

SYSTEM ACCESS INFORMATION FOR SALE ON AN UNDERGROUND FORUM

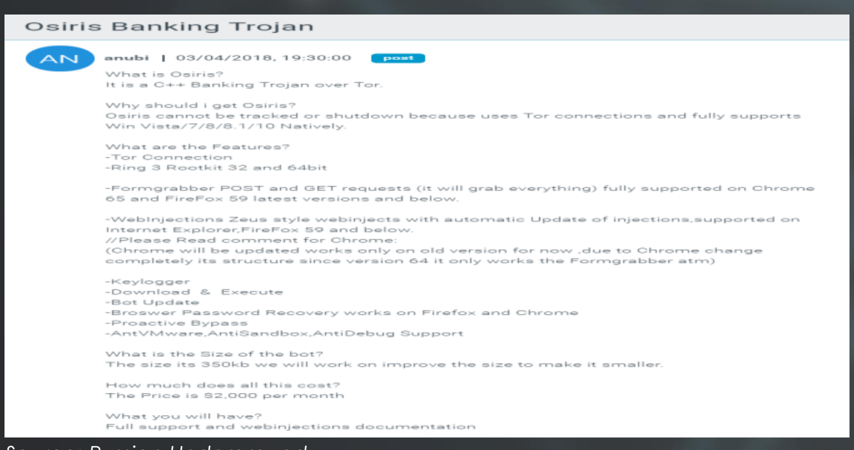
Over the course of the recent weeks, SenseCy analysts have detected numerous underground trade offers in system access information published by a Spanish-speaking threat actor dubbed KelvinSecTeam. The mentioned systems range from GPS vehicle-tracking and insurance companies systems, to electric power and transport systems. As a proof, the threat actor provided screenshots of the records accessible within the systems, showing user databases, confidential documents, personnel photographs, and many more. Based on our tracking of this threat actor in the past years, we believe that by using his high technical capabilities, he was able to identify vulnerable elements in multiple systems and hack into them. **LEARN MORE**



Source: Russian Underground Forum

WPA2 FLAW LEADING TO CRACKING OF WI-FI PASSWORDS IS VIGOROUSLY DISCUSSED ON THE UNDERGROUND

Recently, a new attack method for cracking Wi-Fi network passwords was discovered. By using it, a hacker can obtain the Pairwise Master Key Identifier (PMKID), and decrypt the Wi-Fi password using a brute-force attack. Since the PMKID is received as part of the initial connection attempt (an attacker does not need to wait until a user connects to a Wi-Fi network), we spotted vigorous discussions on underground forums about this attack, indicating a great deal of interest from cybercriminals. The posted information indicates active attack attempts were already carried out. **LEARN MORE**



Source: Russian Underground

OSIRIS - NEW VARIANT OF THE KRONOS BANKING TROJAN DETECTED IN THE WILD

In recent weeks, cyber campaigns utilizing a new variant of the Kronos banking Trojan, called Osiris, were observed in-the-wild. SenseCy analysts were following the sales thread of the Osiris Trojan, posted on a prominent underground forum, since April 2018. However, until the recent identification, Osiris was treated with a great deal of doubt and considered unreliable by the hacking community. The publications about the similarity of Osiris to the Kronos malware led to the resurgence of the discussions regarding Osiris, which in our assesment may lead to expansion of attacks employing this Trojan. **LEARN MORE**

Source: Social Media

LULZSEC_ITA GROUP HACKED THE SERVERS OF OSPEDALE S. ANDREA HOSPITAL IN ROME

During the last month, here at SenseCy we observed a noteworthy cyber-attack conducted by the Italian hacktivist group LulzSec_ITA, in which thousands of records were compromised. The attackers successfully exfiltrated the databases hosted on the servers of the Ospedale S. Andrea hospital, in Rome. According to our analysis of the incident, we assess with medium confidence that the hackers exploited a vulnerability in a plugin of the Joomla CMS utilized by the hospital's website. In the past, LulzSec_ITA group has carried out mainly politically-motivated, high-profile attacks, publishing sensitive information online. Recently, the group has made a comeback on the Italian threat landscape. **LEARN MORE**

TERM OF THE MONTH: PROCESS DOPPELGÄNGING

"A recently discovered malware evasion technique. Process Doppelgänging is a fileless code injection attack, designed to bypass detection by AV engines that resembles another technique called Process Hollowing. However, Process Doppelgänging utilizes the NTFS Transactions Windows mechanism, when two key distinct features are used together to mask the loading of a modified executable. As a result, a process is created from the modified executable, while deployed security mechanisms are not triggered."

The information contained in this report is provided by SenseCy on an "as is" basis, and to the full extent permissible by applicable law, SenseCy does not make any warranties, express or implied, including, without limitation, those of merchantability and fitness for a particular purpose, any warranties as to the accuracy, completeness, quality or adequacy of any information, conclusions set out in this report and any translations therein. All materials included in this report were collected by using legal Open Source intelligence methodologies and supporting technologies. This report does not include interrogation of any specific entity and/or individual. The reader assumes sole responsibility for the selection of this report to achieve its intended results.
Copyright ©SenseCy 2018 | You are receiving this newsletter because you asked to subscribe. To stop receiving these emails, please reply to this email with the subject line "Unsubscribe".