MARCH, 2018
EDITION 15

THE MONTHLY

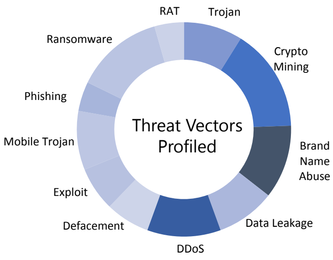
CYBER THREAT INSIDER

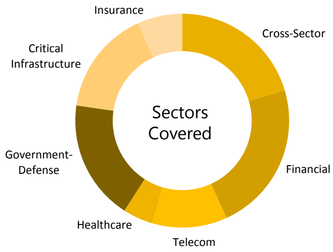
SenseCy
A VERINT Company

POWERED BY WEBINT 7

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:





HOW LONG DOES IT TAKE TO EXPLOIT A VULNERABILITY?

In the past year, the number of disclosed vulnerabilities (14,712) reached an all-time peak in all of cyber-history – twice as high as the two previous years: 6,480 vulnerabilities were discovered in 2015, and 6,447 in 2016. A tremendous number of systems, hardware and firmware was found to be vulnerable, and many of the flaws can have severe consequences and open the front door to hacking into high-profile networks.

When it comes to fixing bugs, it can take time from the discovery of the vulnerability until the manufacturer issues a patch. However, the main issue with vulnerability patching is not the vendor's domain, but lies within the company's remediation gap – i.e. the protracted amount of time it takes to implement the patch in the company's systems.

According to a 2015 Kenna Security's Remediation Gap report, most companies take an average of 100-120 days to patch vulnerabilities, while the probability of a vulnerability being exploited hits 90% between 40-60 days after discovery. These numbers translate into avoidable security incidents where attackers exploit vulnerabilities that had been patched weeks and sometimes months before the attack.

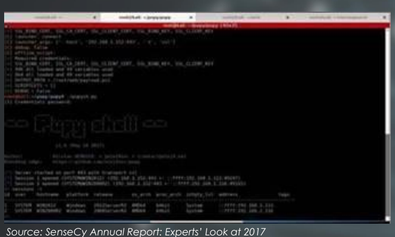
In the SenseCy annual report, we chose to inspect exploit-based attacks in terms of the time it takes from the disclosure of the vulnerability through the development of a suitable exploit, which frequently takes place on underground hacking communities, to its usage in the wild. A better understanding of this time frame and its fluctuations may assist organizations in their vulnerabilities-mitigation plan and mark the critical time point after which the risk of attack on an unpatched system increases exponentially.

READ MORE ON OUR BLOG

Source: SenseCy Annual Report: Experts' Look at 2017

HIGH PROFILE DATA LEAKAGES WERE A PROMINENT TREND IN 2017

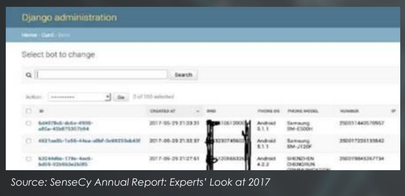
This year, in addition to the 'traditional' type of data leaks (Equifax, Uber, etc.), we witnessed data leakages from high-profile sources, i.e. government and intelligence agencies. In these attacks, confidential information with a high damage potential was stolen and published online. Two prominent attacks of this type took place in 2017: the first was the leak of the NSA hacking tools by the Shadow Brokers hacking group. The second attack was known by the name Vault 7, and included a series of publications by WikiLeaks that includes information on the capabilities, methods and tools used by the CIA. LEARN MORE



Source: SenseCy Annual Report: Experts' Look at 2017

PROLIFERATION OF NATION-STATE ATTACK TOOLS OCCURRED AS A RESULT OF THE DATA LEAKAGES

The data leakage of confidential material from governmental agencies led to the transition of highly-sophisticated attack tools from the exclusive use of nation-states to the hands of cybercriminals, who wasted no time adopting them to suit their own agendas. Each batch of cyber materials leaked by Shadow Brokers led to extensive discussions on the hacking communities SenseCy monitors, dealing with the modification, trade and methods of employment of the leaked exploits and tools, effectively serving as fertile ground for a whole new arsenal of cyber-ammunition by cybercriminals, such as financial malware and ransomware distribution. LEARN MORE



Source: SenseCy Annual Report: Experts' Look at 2017

NEW ATTACK VECTORS AT THE SERVICE OF CYBERCRIMINALS, AFTER THE DECLINE OF EXPLOIT KITS

Unsurprisingly, in a great deal of attacks, we continue to see the exploitation of malicious files distributed by email, frequently in .doc or .pdf formats. JavaScript files have also become extremely popular among cybercriminals in recent years and there are many services on the underground offering to create such files. Additionally, several new banking Trojans targeting Android devices, such as the Loki Bot, Red Alert bot and others emerged in 2017 on the Russian underground. Finally, the sharp rise in the value of Bitcoin and other cryptocurrencies that marked the end of 2017, has increased the motivation of cybercriminals to develop and spread mining malware. As a result, we have witnessed a sharp rise in the trade and distribution of miners. LEARN MORE

Source: SenseCy Annual Report: Experts' Look at 2017

DARKNET DEVELOPMENTS - NATURE ABHORS A VACUUM

A major event from 2017 was the take down of known and well-established Darknet markets and the rapid rise of others replacing them. During 2017, the AlphaBay and Hansa marketplaces were taken down by law enforcement authorities. Dream Market (initially founded in 2013) soon replaced the closed markets in the leading position for the trade of illegal goods, offering all sorts of drugs, as well as digital goods, leaked records, and porn. LEARN MORE

TERM OF THE MONTH:

BEC ATTACK

"A Business Email Compromise (BEC) attack involves impersonating company employees and using social engineering techniques to perform fraudulent money transactions. Companies with international operations are usually targeted, as they perform hefty wire transfer payments regularly. The attackers usually attempt to impersonate company executives with access to corporate finance, principally CFOs but also CEOs, COOs and other C-level Executives."