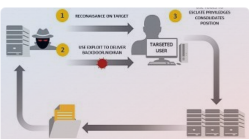
Suckfly Cyber-Espionage Group Targets Indian Government and Private Companies

Suckfly uses OLE exploits and the Nidiran backdoor

May 18, 2016 00:10 GMT · By Catalin Cimpanu · Comment · Share:

A cyber-espionage group called Suckfly is targeting governments and big enterprises, mainly located in India, using a backdoor named Nidiran, a credential dumping tool dubbed Hacktool, Windows OLE exploit CVE-2014-6332, and stolen digital certificates.


1 RECONAISANCE ON TARGET
2 USE EXPLOIT TO DELIVER BACKDOOR.NIDIRAN
3 ESCLATE PRIVILEDGES CONSOLIDATES POSITION
TARGETED USER

Suckfly group mode of operation

The group first came to Symantec's attention when, in March, it was caught stealing digital certificates from various South Korean companies.

A few months later, while investigating clues left behind by the group, Symantec experts claimed to have discovered Suckfly activity going back as early as April 2014.

Suckfly group focused on Indian targets

The group mainly targeted Indian companies, but researchers found hacked businesses in Saudi Arabia as well. Symantec says it discovered the group targeted two Indian government organizations, a large e-commerce company, one of the country's biggest financial groups, one of its top five IT companies, a shipping vendor, and a US-based healthcare provider for various Indian companies.

Except one privately owned company, the group spent more time attacking the two Indian government agencies than anyone else.

"There is no evidence that Suckfly gained any benefits from attacking the government organizations, but someone else may have benefited from these attacks," Symantec's Joe DiMaggio reported. "The nature of the Suckfly attacks suggests that it is unlikely that the threat group orchestrated these attacks on their own."

Suckfly uses APT-style tactics

Symantec's analysis of Suckfly's mode of operation reveals cyber-warfare tactics employed by many APT and economic espionage groups.

Suckfly attacks start with phishing emails that deliver boobytrapped documents. These files exploit CVE-2014-6332 to infect the target with the Nidiran backdoor, which attackers use to install Hacktool, a password dumping utility.

Crooks then use these passwords to scout and search the local network, gather any potentially interesting data and use the backdoor again to send it off to their servers.

Symantec noted that these attacks took place only on weekdays, when the group was sure to find people at work to read the spear-phishing emails.

At the moment, security researchers could not exactly tell if the group is state-sponsored or not.

#India, #Suckfly, #cyber-espionage, #APT, #backdoor

HOT RIGHT NOW

US Company Develops Surveillance Cameras That Could Help Detect COVID-19: Cameras feature a thermal system to check body temperature

Working from Home Amid COVID-19 a No-No for Apple Staff Due to FBI-Like Secrecy: Employees required to work from home due to COVID-19

Purism Announces Discounts For Librem Linux Laptops: The laptops will ship when they are back in stock

Microsoft Announces Mysterious March 30 Event: The whole thing will obviously take place online

Microsoft Reveals All the Hardware Inside the Xbox Series X Console: Three perks define it: power, speed, and compatibility

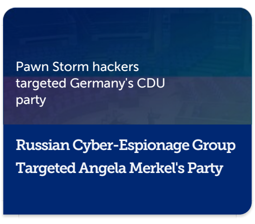
Coronavirus Tracker Infects Smartphones with Ransomware: Virus-tracking app coming with a virus of its own

Microsoft Launches a Free COVID-19 Tracker for Desktop and Mobile: The app is available on Bing and also includes news

Click to load comments

This enables Disqus, Inc. to process some of your data. Disqus privacy policy

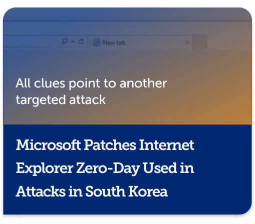
Related Stories


Pawn Storm hackers targeted Germany's CDU party

Russian Cyber-Espionage Group Targeted Angela Merkel's Party

Officials investigating hack at navy ship builder

South Korea Accuses North Korea of Hacking Defense Contractor


All clues point to another targeted attack

Microsoft Patches Internet Explorer Zero-Day Used in Attacks in South Korea

Russian hackers suspected, no official accusations yet

Swiss Defense Ministry Hit by Cyber-Attack

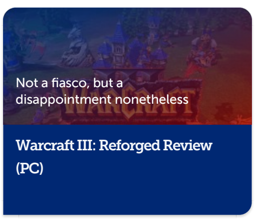
Group was active and remained secret for at least nine years

Security Firm Exposes Secret Iranian Cyber-Espionage Campaign

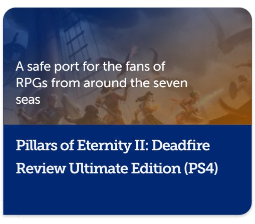
Fresh Reviews

The best Dragon Ball game for newcomers to the series

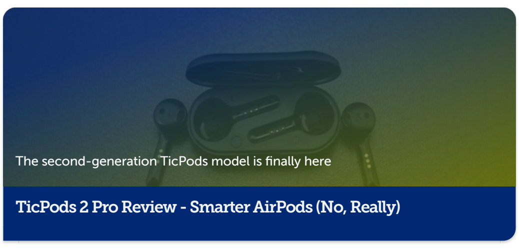
Dragon Ball Z: Kakarot Review (PS4)


Not a fiasco, but a disappointment nonetheless

Warcraft III: Reforged Review (PC)


A safe port for the fans of RPGs from around the seven seas

Pillars of Eternity II: Deadfire Review Ultimate Edition (PS4)

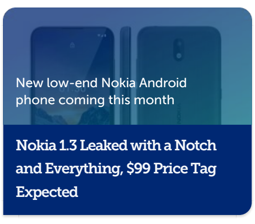

The second-generation TicPods model is finally here

TicPods 2 Pro Review - Smarter AirPods (No, Really)

The most complete and balanced episode in the series

Sniper Ghost Warrior Contracts Review (PS4)

Latest News


New low-end Nokia Android phone coming this month

Nokia 1.3 Leaked with a Notch and Everything, $99 Price Tag Expected

A new update now available for Windows 10 version 1809

Windows 10 Cumulative Update KB4541331 Fixes Blue Screen Error During Upgrade

US AG calls for crackdown on coronavirus scams

US Government Goes After Hackers Exploiting COVID-19 Fears

The company tries to deal with a huge boost in demand

Microsoft Throttles Non-Essential Office 365 Features to Avoid Outages

Coronavirus impact still limited, the company says

So It Begins: Dixons Carphone Closes All Standalone Stores, 2,900 Left Jobless

Cameras feature a thermal system to check body temperature

US Company Develops Surveillance Cameras That Could Help Detect COVID-19

Google Cloud Next postponed until a later date

Google Postpones Tech Conference (Even the Digital Version) Due to COVID-19

GitHub for mobile devices is now available for download

GitHub Officially Launches Android and iPhone App

The update brings diplomatic missions and much more

X4: Split Vendetta Expansion Launches on March 31 Alongside 3.0 Update