SECURITYWEEK
INTERNET AND ENTERPRISE SECURITY NEWS, INSIGHTS & ANALYSIS

Researchers Disrupt Iranian Cyberespionage Campaign

By Eduard Kovacs on June 29, 2016

in Share 33 G+1 4 Tweet 推薦 17 RSS

Researchers at Palo Alto Networks have managed to disrupt an Iran-linked cyberespionage campaign targeting governments and businesses from all around the world.

The security firm reported in May that it uncovered a new malware family that had been used in espionage operations since at least 2007 by a group believed to be located in Iran. The malware, dubbed “Infy,” remained under the radar because it had only been used in highly targeted attacks.

After it published its report on Infy, Palo Alto Networks started working with the entities that hosted the threat actor’s command and control (C&C) infrastructure in an effort to take control of their domains.

Following the disclosure, the attackers moved their C&C domains to new IP addresses and released a new version of the malware, but these types of activities were conducted regularly even before the security firm released its findings to the public. However, the encoding technique and key used by the attackers, which allowed investigators to identify Infy samples, remained unchanged, which led experts to believe that the threat group was unaware of their report.

Palo Alto Networks initially managed to take control of all but one of the C&C domains used by the attackers. This prevented the group from continuing to steal information from most of the victims.

However, the cyberspies did not give up and used the remaining C&C domains they controlled in an attempt to revive the campaign. In the end, the security firm managed to sinkhole all the domains and completely shut down the campaign.

An analysis of the sinkholed domains led to the discovery of over 450 malware agents installed on 326 systems spread across 35 countries in North America, Europe, Asia (particularly the Middle East) and Australia. Experts noted that many of the victims were Iranian citizens.

While there are more than 40 variants of the Infy malware, researchers say there are only two major versions. The original Infy has been used to infect more than 90 percent of victims, while the more sophisticated version, Infy M, has been mainly leveraged against high-value targets.

The latest Infy variant, which attackers started deploying after most of their C&C domains were hijacked, no longer records videos, but continues to steal files that could hold valuable information. The new version also checks for the presence of antivirus products from Kaspersky, Trend Micro and Avast.

While Palo Alto Networks has managed to disrupt this campaign, researchers expect the threat actor to return soon.

in Share 33 G+1 4 Tweet 推薦 17 RSS

Previous Columns by Eduard Kovacs:
» Noodles & Company Confirms Payment Card Breach
» Russia-Linked Cyberspies Target Google Accounts
» Researchers Disrupt Iranian Cyberespionage Campaign
» Critical Flaws Expose Symantec Customers to Remote Attacks

Google™ Custom Search

Most Recent Most Read
» Hackers Use Basic Tools After Breaching Your Network

» Mining Industry Increasingly Targeted by Threat Actors

Tags: NEWS & INDUSTRY Virus & Threats

» Overwhelming Majority of Android Devices Don't Have Latest Security Patches

» Noodles & Company Confirms Payment Card Breach

» Historical Perspective on Dark Web Sale of 10 Million Health Records

» The Increasing Importance of Security Analytics

» Russia-Linked Cyberspies Target Google Accounts

» New X25519 Cipher Throws Enterprise Surveillance for a Loop

» Researchers Disrupt Iranian Cyberespionage Campaign

» Critical Flaws Expose Symantec Customers to Remote Attacks

» The Great Analyst Debate Over Consumer IAM

DISCUSSION

PEOPLE RECENT POPULAR

Recent Comments

Jeff Chapman
Deciding which platform to buy (Android versus iOS) means you're going to be making some kind of sacrifice. If security is a concern of yours (and it should be), buying an iPhone makes a lot of sense.
Overwhelming Majority of Android Devices Don't Have Latest Security Patches · 11 hours ago

brownj00
Yes, I am reminded of a recent news story where Facebook founder Mark Zukerberg's social media accounts on twitter, instagram, and pinterest were all compromised because he reused the same...
TeamViewer Denies Breach After Users Get Hacked · 12 hours ago

BeSecure
If 74 percent of BlackHat attendees say users were their biggest headache, they what are they doing about it? A culture that embraces information security as one of its main tenants begins with...
What Keeps Security Professionals Up at Night? Their Users · 1 day ago

community on DISQUS

Popular Topics
- Information Security News
- IT Security News
- Risk Management
- Cybercrime
- Cloud Security
- Application Security
- Smart Device Security

Security Community
- IT Security Newsletters
- Suits and Spooks
- ICS Cyber Security Conference
- CISO Forum
- InfosecIsland.Com

Stay Intouch
- Twitter
- Facebook
- LinkedIn Group
- Cyber Weapon Discussion Group
- RSS Feed
- Submit Tip
- Security Intelligence Group

About SecurityWeek
- Team
- Advertising
- Events
- Writing Opportunities
- Feedback
- Contact Us

Wired Business Media