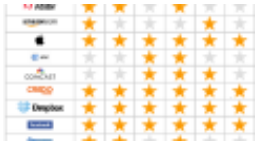
Threatpost – English – Global – threatpost.com

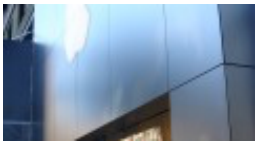
- Categories
  - Category List
    - Apple
    - Cloud Security
    - Compliance
    - Critical Infrastructure
    - Cryptography
    - Government
  - Category List
    - Hacks
    - Malware
    - Microsoft
    - Mobile Security
    - Privacy
  - Category List
    - SMB Security
    - Social Engineering
    - Virtualization
    - Vulnerabilities
    - Web Security
  - Authors
    - Dennis Fisher
    - Michael Mimoso
    - Christopher Brook
    - Brian Donohue
    - Anne Saita
  - Additional Categories
    - Slideshows
  - The Kaspersky Lab News Service
- Featured
  - Authors
    - Dennis Fisher
    - Michael Mimoso
    - Christopher Brook
    - Brian Donohue
    - Anne Saita
    - Guest Posts
  - The Kaspersky Lab News Service

Featured Posts

All

 Snowden, Surveillance Prompt Tech Companies to…

 Critical Infrastructure Companies Continue to Patch…

 Apple Releases OS X 10.9.3, Fixes…

- Podcasts

Latest Podcasts

All

 Threatpost News Wrap, May 9, 2014

 Threatpost News Wrap, April 25, 2014

 Kurt Baumgartner on APT Attacks in…

 Eugene Kaspersky on Critical Infrastructure Security

 Threatpost News Wrap, April 11, 2014

 Mike Mimoso on CanSecWest and Pwn2Own

Recommended

- Threatpost News Wrap, February 21, 2014
- How I Got Here: Jeremiah Grossman
- Chris Soghoian on the NSA Surveillance and Government Hacking
- Adrian Stone on BlackBerry Security, Privacy and the Challenges of BYOD

The Kaspersky Lab Security News Service

- Videos

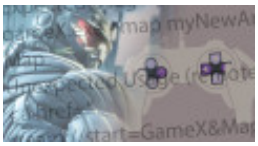
Latest Videos

All

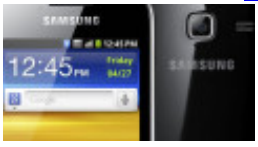
 Twitter Security and Privacy Settings You...

 The Biggest Security Stories of 2013

 Jeff Forristal on the Android Master-Key...

 Researchers Discover Dozens of Gaming Client...

 Mozilla Drops Second Beta of Persona...

 Vulnerabilities Continue to Weigh Down Samsung...

Recommended

- Twitter Security and Privacy Settings You Need to Know
- Lock Screen Bypass Flaw Found in Samsung Androids
- Facebook Patches OAuth Authentication Vulnerability
- Video: Locking Down iOS

The Kaspersky Lab Security News Service

Search

- Twitter
- Facebook
- Google
- LinkedIn
- YouTube
- RSS

05/19/14 8:15
XMPP Mandating Encryption on Messaging Service Operators - http://t.co/EyqxdYWPYQ

-
-

Welcome > Blog Home>Malware > Iranian Hackers Target US Defense Contractors

- Share on Twitter

- Share on Facebook
- Google +1
- Share on LinkedIn
- Submit this to Reddit

1

Iranian Hackers Target US Defense Contractors

Follow @mike_mimoso by Michael Mimoso May 13, 2014 , 2:07 pm

An Iranian hacking group has moved from politically motivated website defacements to a new specialty – cyberespionage.

The group known as the Ajax Security Team has been outed as the perpetrators of a number of espionage operations against U.S.-based defense contractors in addition to targeting Iranians using software that bypasses the country's Internet filters.

Related Posts

Zeus' Reach Expands With New Webinjects

May 14, 2014 , 3:14 pm

Points of Sale Poorly Secured, Facing Sophisticated Attacks

May 12, 2014 , 12:31 pm

Sefnit Accomplices Account for Spike in Malware Infections

May 7, 2014 , 2:37 pm

Security company FireEye reported today that the Ajax Security Team uses custom-built malware in its attacks, and is adept at social engineering as a means of infecting targets.

“The transition from patriotic hacking to cyber espionage is not an uncommon phenomenon. It typically follows an increasing politicization within the hacking community, particularly around geopolitical events,” researchers Nart Villeneuve, Ned Moran, Thoufique Haq and Mike Scott wrote today. “This is followed by increasing links between the hacking community and the state, particularly military and/or intelligence organizations.”

Iranian hacker groups have long been suspected in the attacks against Saudi Aramco using wiper malware known as Shamoon which destroyed more than 30,000 workstations at the oil plant in Saudi Arabia. FireEye said Iran’s offensive hacking capabilities have evolved since the country’s nuclear and political resources were targeted by Stuxnet and Flame.

The attackers, like most in advanced persistent threat-style campaigns, try to trick victims into either installing malware on computers or giving up credentials. In a campaign disclosed by FireEye called Operation Saffron Rose, the Ajax Security Team used email, private messages over various social networks, phony log-in pages and peddling of anticensorship software spiked with malware that allows them to monitor victims and exfiltrate data from their machines.

The lure in attacks against the defense industrial base, for example, was a phony registration page impersonating the IEE Aerospace conference. The group registered a domain similar to the legitimate conference domain and emailed targets a link to their site. Once on the site, a popup directs the victim to install proxy software in order to access the site and register. The software is malicious, FireEye said.

The attackers also used phishing emails looking to gather up credentials for a variety of online services such as Outlook Web Access and VPN logins.

FireEye said the hackers use homegrown malware they call Stealer. A dropper leaves behind malware called IntelRS.exe and other components that encrypt stolen data, steal browser information such as bookmarks and history, steal data via FTP and drop keylogger and screenshot-grabbing tools. The malware also collects system information such as running processes, IP addresses and lots more.

The operation dates back to late last year, and was active as recently as April 8, FireEye said.

FireEye said it has information on 77 victims from one of the attackers’ command and control servers. Most of the victims’ machines in the attacks peddling spiked anticensorship tools were set to Iran Standard Time or had a Persian language setting.

“We believe that attackers disguised malware as anti-censorship tools in order to target the users of such tools inside Iran as well as Iranian dissidents outside the country,” the researchers said.

FireEye also identified the founding members of the team, hackers known as HUrr!c4nE and Cair3x, both of whom were known for website defacements and were members of different Iranian hacker forums. The researcher said the pair, including others prominent on Iranian forums have become increasingly political, targeting the U.S. and Israel in particular in blogposts. Their activity, however, has been minimal since early this year, FireEye said.

“While the objectives of this group are consistent with Iran’s efforts at controlling political dissent and expanding offensive cyber capabilities, the relationship between this group and the Iranian government remains inconclusive,” the researchers said. “For example, the Ajax Security Team could just be using anti-censorship tools as a lure because they are popular in Iran, in order to engage in activities that would be considered traditional cybercrime.”

1
Categories: Malware

Comment (1)

1.  *Soufiane Tahiri* May 14, 2014 @ 4:33 am
   1

   Regarding the analysis given by FireEye team , Ajax Secuiy Team is not that advanced team the use of such a “simple” malware leave us think they are more kids playing around with code rather than a real “government actors” there is no way to compare the complexity of real APTs with this said “stealer” !

   Reply ↓

Leave A Comment

Your email address will not be published. Required fields are marked *

Name NAME_FULL

Email EMAIL_ADDRESS

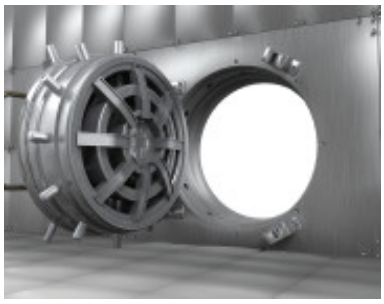
Comment UNKNOWN_TYPE

You may use these HTML tags and attributes: `<a href="" title=""> <abbr title=""> <acronym title=""> <b> <blockquote cite=""> <cite> <code> <del datetime=""> <em> <i> <q cite=""> <strike> <strong>`

Post Comment

- [ ] Notify me of follow-up comments by email.
- [ ] Notify me of new posts by email.

Recommended Reads



- Share on Twitter
- Share on Facebook
- Google +1
- Share on LinkedIn
- Submit this to Reddit

1
May 14, 2014 , 3:14 pm
Categories: Malware

Zeus’ Reach Expands With New Webinjects

by Michael Mimoso

The peer-to-peer version of Zeus was especially busy in the first quarter with infections reported by banks in 10 countries that previously had eluded Zeus’ reach.

Read more...

- Share on Twitter
- Share on Facebook
- Google +1

- Share on LinkedIn
- Submit this to Reddit

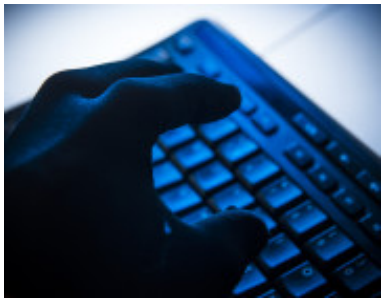
0
May 12, 2014 , 12:31 pm
Categories: Malware

Points of Sale Poorly Secured, Facing Sophisticated Attacks

by Brian Donohue

As the sophistication and deployment of PoS malware increases, organizations struggle to defend against even simple attacks.

Read more...



- Share on Twitter
- Share on Facebook
- Google +1
- Share on LinkedIn
- Submit this to Reddit

0
May 7, 2014 , 2:37 pm
Categories: Microsoft

Sefnit Accomplices Account for Spike in Malware Infections

by Michael Mimoso

Microsoft's latest Security Intelligence Report identifies two malware families, Rotbrow and Brantall, previously thought to be benign that have been dropping the Sefnit botnet.

Read more...

Top Stories

U.S. Indicts Five Chinese Army Officers for Alleged Cyberespionage Operations

May 19, 2014 , 11:30 am

FTC Settles With Fandango, Credit Karma Over SSL Issues in Mobile Apps

March 28, 2014 , 2:30 pm

AOL Email Hacked by Spoofers to Send Spam

April 22, 2014 , 4:20 pm

Targeted Attacks Exploit Microsoft Word Zero Day

March 24, 2014 , 3:20 pm

Second NSA Crypto Tool Found in RSA BSafe

March 31, 2014 , 3:59 pm

Threatpost News Wrap, April 11, 2014

April 11, 2014 , 12:06 pm

Passcode Bypass Bug and Email Attachment Encryption Plague iOS 7.1.1

May 5, 2014 , 4:59 pm

Eugene Kaspersky on Critical Infrastructure Security

April 16, 2014 , 11:00 am

LinkedIn Goes After Email-Scraping Browser Plug-In

April 1, 2014 , 2:54 pm

The Final Say

From Kaspersky Blogs

[Three ways to protect virtual machines....]

To protect or not to protect virtual machines – that was the question, asked by many. But the answer's been the same all along: to protect. The more crucial question is how to protect. I've already wr...

Read more...

Blog: The Bitcoin 2014 Conference - Are Crypto-Cur...

As the Bitcoin 2014 conference is unwinding here in Amsterdam today, I have to admit that I am impressed by how the crypto-currency community is making rapid steps towards reaching maturity....

Read more...

Five Worst Mistakes You Can Make on Facebook

What Facebook habits make you vulnerable and how to avoid them.

Read more...

Threat landscape in the era of targeted attacks

Last week, Kaspersky Lab hosted a webinar to discuss the threat landscape in the era of targeted attacks. Here's a summary and slides from this event.

Read more...

Worry-free holidays...

Sooner or later another school year will draw to a close. The exams will be finished and dissertations defended. It’s time to relax and think about a vacation. How about the beach? It would be great i...

Read more...

Authors

Dennis Fisher
Michael Mimoso
Christopher Brook
Brian Donohue
Anne Saita