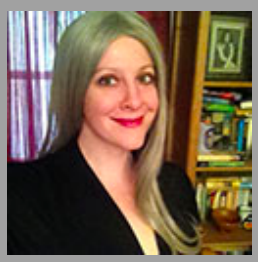
Attacks/Breaches

2/23/2016
06:00 PM



Sara Peters
News

Connect Directly

0 comments

Operation Dust Storm Hackers Set Sights On Japan's Critical Infrastructure

Japanese energy, oil/gas, and transportation industries the target of stealthy, patient cyber-espionage group.

A threat group that has attacked a variety of targets including US defense agencies since 2010, has recently zeroed in all efforts on Japanese critical infrastructure. Though they have not yet been "destructive or disruptive," the cyber espionage group has been quietly, persistently lurking within Japan's power, oil/gas, construction, finance, and transportation industries, according to researchers at the Cylance SPEAR Team.

Dubbed Operation Dust Storm by researchers, the attackers' tools of choice are mostly second-stage backdoors and their activities are related to current events. In 2011, early in the group's evolution, they targeted the US defense sector by using phishing lures related to the death of Libyan Prime Minister Muammar Gaddafi. More recently, in 2015, group compromised investment arm of a Japanese automaker, implanting a second-stage backdoor (via an existing backdoor) two weeks before 11 Japanese autoworker unions demanded a monthly raise of 6,000 yen.

Their goals thusfar appear to be reconaissance and long-term espionage. "At this time, SPEAR does not believe the attacks were meant to be destructive or disruptive," according to the report. "However, our team believes that attacks of this nature on companies involved in Japanese critical infrastructure and resources are ongoing and are likely to continue to escalate in the future."

The group has managed to maintain persistence and stay under the radar, by registering new domain names, taking advantage of dynamic DNS, and using a variety of customized backdoors -- particularly second-stage backdoors with hard-coded proxy addresses and credentials, as well as Android backdoors. Their mobile malware initially only forwarded SMS and call data to command-and-control servers, then added the ability to enumerate and exfiltrate specific files from devices. Those efforts to stay ahead of security tools have been largely successful.

According to the report: "No antivirus vendors seem to reliably detect most of the variants SPEAR identified."

Sara Peters is Senior Editor at Dark Reading and formerly the editor-in-chief of Enterprise Efficiency. Prior that she was senior editor for the Computer Security Institute, writing and speaking about virtualization, identity management, cybersecurity law, and a myriad ... View Full Bio

Comments

Newest First | Oldest First | Threaded View

Be the first to post a comment regarding this story.

Subscribe to Newsletters

Live Events Webinars

UBM Tech

More UBM Tech Live Events

Hear SIP Trunking Savings & Options at Enterprise Connect

Get UC & Collaboration Insights at Enterprise Connect

Come to Interop Las Vegas, May 2 - 6, 2016

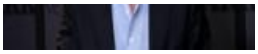
White Papers

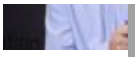
- Measuring Mobile Security Risk on Financial Sector Devices
- 5 Evergreen Insights: Mobile Security in a BYOD World
- 2015 Shadow Data Report
- 2015 Strategic Security Survey
- [Report] Defending Data

More White Papers

Video

Cartoon Contest





Write a Caption, Win a Starbucks Card! Click Here

All Videos

Latest Comment: This comment is waiting for review by our moderators.

Cartoon Archive

Current Issue

E-Commerce Security: What Every Enterprise Needs to Know

The mainstream use of EMV smartcards in the US has experts predicting an increase in online fraud. Organizations will need to look at new tools and processes for building better breach detection and response capabilities.

Download This Issue!

Back Issues | Must Reads

Flash Poll

What's missing from your incident response plan? (Pick all that apply.)

- [ ] Access to activity logs
- [ ] An up-to-date network diagram
- [ ] Blueprint for public disclosure
- [ ] Hostname-IP address maps
- [ ] IR fire drills before the event

- [ ] Plan for finding malicious files after the breach
- [ ] We don't have an incident response plan
- [ ] Other (Please explain in the comments)

Submit

All Polls

Slideshows

FBI Vs. Apple: Privacy Syllabus

1 comments | Read | Post a Comment

Cybercrime And Hacking Atlas 7

20 Cybersecurity Startups To Watch In 2016 2

More Slideshows

Twitter Feed

Jennifer Jessup @jjessup44 6h

Brand new description for the Hands-On Hacking workshop @Interop, May 2. ow.ly/YIpEI @DarkReading

Retweeted by Ruby Betten

Show Summary

Ericka Chickowski @ErickaChick 10 Feb

Is the cybersecurity bubble about to burst? A look at either side of the debate ow.ly/YacuL @DarkReading pic.twitter.com/mH2DBhKsaV

Retweeted by vgtero

Bug Report

Enterprise Vulnerabilities
From DHS/US-CERT's National Vulnerability Database

- CVE-2013-7445
  Published: 2015-10-15
  The Direct Rendering Manager (DRM) subsystem in the Linux kernel through 4.x mishandles requests for Graphics Execution Manager (GEM) objects, which allows context-dependent attackers to cause a denial of service (memory consumption) via an application that processes graphics data, as demonstrated b...
- CVE-2015-4948
  Published: 2015-10-15
  netstat in IBM AIX 5.3, 6.1, and 7.1 and VIOS 2.2.x, when a fibre channel adapter is used, allows local users to gain privileges via unspecified vectors.
- CVE-2015-5660
  Published: 2015-10-15
  Cross-site request forgery (CSRF) vulnerability in eXtplorer before 2.1.8 allows remote attackers to hijack the authentication of arbitrary users for requests that execute PHP code.
- CVE-2015-6003
  Published: 2015-10-15
  Directory traversal vulnerability in QNAP QTS before 4.1.4 build 0910 and 4.2.x before 4.2.0 RC2 build 0910, when AFP is enabled, allows remote attackers to read or write to arbitrary files by leveraging access to an OS X (1) user or (2) guest account.
- CVE-2015-6333
  Published: 2015-10-15
  Cisco Application Policy Infrastructure Controller (APIC) 1.1j allows local users to gain privileges via vectors involving addition of an SSH key, aka Bug ID CSCuw46076.

Dark Reading Radio