MalwareMustDie is closed for protest against the NSA

November 10, 2016 By Pierluigi Paganini

http://securityaffairs.co/wordpress/53285/malware/malwaremustdie-closed.html

My Page

The Legendary Blog of MalwareMustDie is closed for protest against NSA hacking trace of educational and public servers of harmless countries.

The Shadow Brokers, the hacker group that hacked NSA hackers, who have previously released NSA hacking tools for anyone to download, published more files containing the IP address of 49 countries that have been hacked by the US National Security Agency. Security experts on several media news are linking these nodes to the activity of Equation Group.

MalwareMustDie (MMD) group has started to focus the attention on the case, since Japan appeared to be the second most hacked country victims in the list, and was not listed as known target in the Equation Group (EQGRP) activities so far.

In the mean time, the result of the EQGRP hacking activity, based on malware used to infect Linux and Solaris platforms, has been reversed and published by CERT Antiy and with full details, except of the hashes that was not shared in their publishment.

Figure 1. The reverse of Linux and Solaris malware used by Equation Group

Researchers in the MalwareMustDie group has started to dig in the details and discovered that several accessible parts of the listed environments during the specific known period are having traces of unknown suspicious malicious codes and activities matched to the period and activity mentioned in several announced publicity. So far the group is currently avoiding public disclosure to what they found.

Following this investigation progress, a new awareness has raised giving the evidence that Universities/Schools, Internet Service Providers (ISP), Public Mail Service, Cable Television Network, a National NIC network, Entertainment network, Government Offices, and maybe more, has been in the risk of violated by the unauthorized access and malicious activity. Since the investigation was based on the list originated from the ShadowBroker's post, the allegedly pointed attacker country's spy entities are assumed responsible for the act.

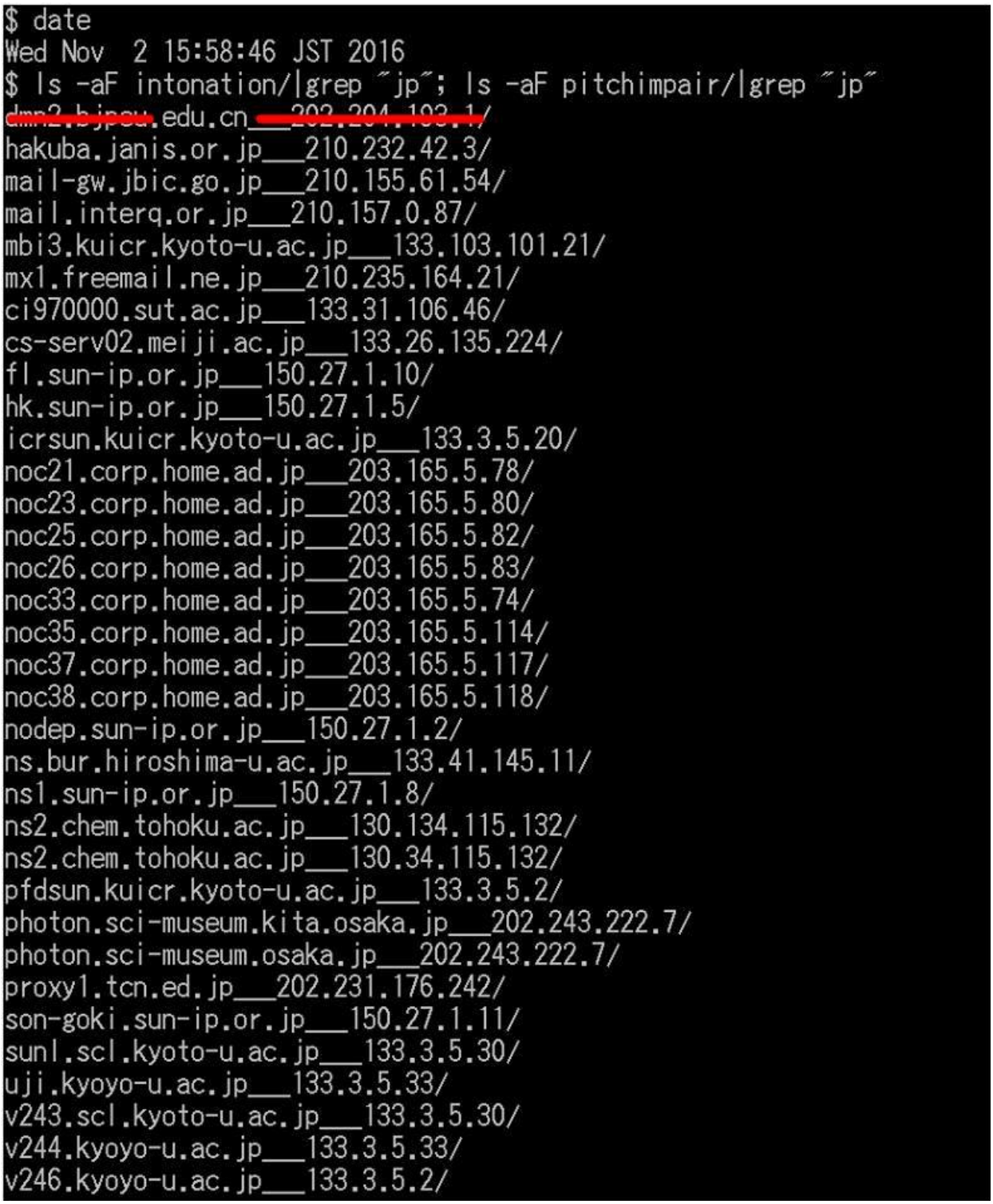
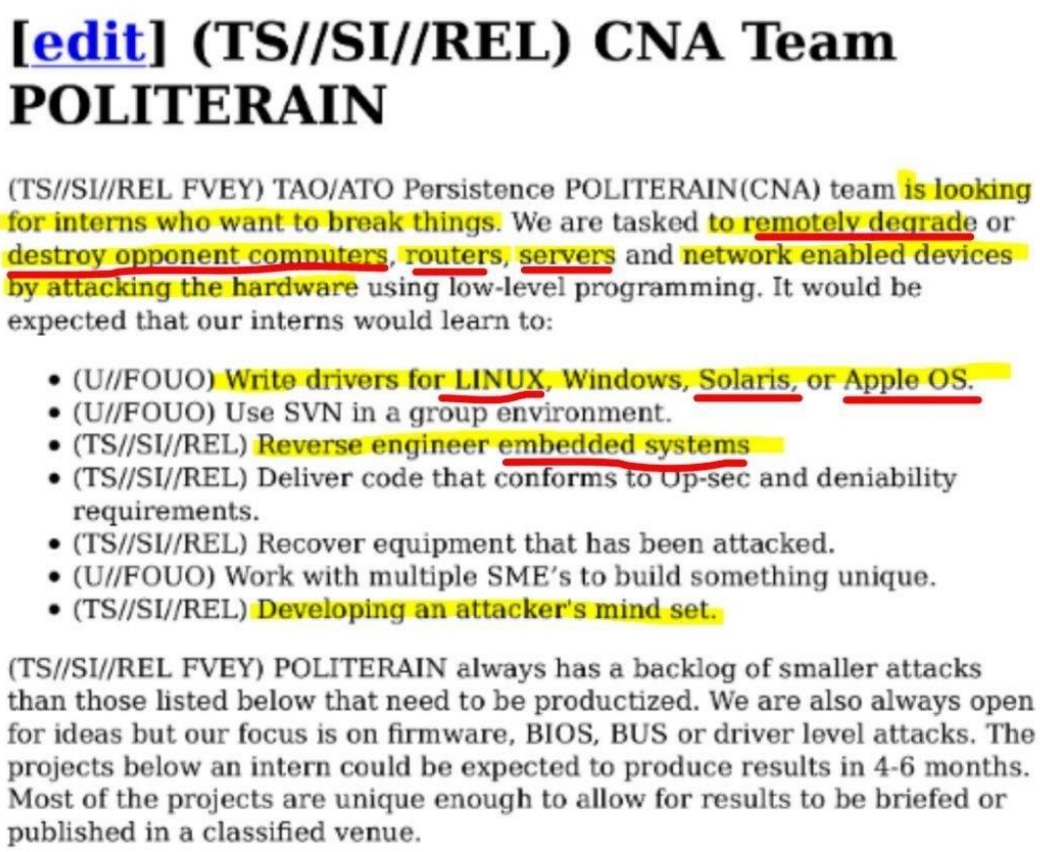


Figure 2. Shadow Broker's list of infected nodes in Japan with PITCHIMPAIR & INNOVATION

According to the usage of the platform, this investigated sad event's fact may also in relation to what Der Spiegel has reported of the leaked NSA documentation in the past:



[edit] (TS//SI//REL) CNA Team POLITERAIN

(TS//SI//REL FVEY) TAO/ATO Persistence POLITERAIN(CNA) team is looking for interns who want to break things. We are tasked to remotely degrade or destroy opponent computers, routers, servers and network enabled devices by attacking the hardware using low-level programming. It would be expected that our interns would learn to:

- (U//FOUO) Write drivers for LINUX, Windows, Solaris, or Apple OS.
- (U//FOUO) Use SVN in a group environment.
- (TS//SI//REL) Reverse engineer embedded systems
- (TS//SI//REL) Deliver code that conforms to Op-sec and deniability requirements.
- (TS//SI//REL) Recover equipment that has been attacked.
- (U//FOUO) Work with multiple SME's to build something unique.
- (TS//SI//REL) Developing an attacker's mind set.

(TS//SI//REL FVEY) POLITERAIN always has a backlog of smaller attacks than those listed below that need to be productized. We are also always open for ideas but our focus is on firmware, BIOS, BUS or driver level attacks. The projects below an intern could be expected to produce results in 4-6 months. Most of the projects are unique enough to allow for results to be briefed or published in a classified venue.

Figure 3. Der Spiegel's published description of the hacking inquiries of NSA

The development of verdict that a friendly country was spotted to violate services of its allied countries, is a very sad pill to swallow, but the traces were there and that is the reality. Driving to the possibility of such level for mass offensive acts using hacking and malware activity would need the approval from the attacker's operative authority and obviously the attacker's government was also known and giving authorization for the act.

As the current conclusion of the investigation development, is started to be formed, consequentially, MalwareMustDie, as an entity against any usage of malicious software (malware) forms, that is known with their anti-malware research and analysis blog that since 4 long years produces research activity against malware, cybercrime and vandalism in Internet using malware, as a legitimate protest, was decided to close their analysis blog in blog.malwaremustdie.org, for an undefined period, leaving on their twitter profile the following statement:

Figure 4. The protest statement of MalwareMustDie against the NSA hacking

"For this reason, MMD blog is closed for an undefined period. USA related entities and researchers' access to direct communication & research is prohibited under the same condition. Furthermore", they continue, "we stop using any of US services or products for our research."

The title of the Blog is clear, and the position of MalwareMustDie it's clear as well: using malware is any activity with any kind of purpose, is just not accepted. "What is BAD stays BAD, no matter who you are. And if we can not do things strictly right, we can never stop "wrong" or "bad" things in the internet". And it's correct, because, really, malware must die.

About the Author: Odisseus

Independent Security Researcher involved in Italy and worldwide in topics related to hacking, penetration testing, and development.

Edited by Pierluigi Paganini

(Security Affairs – MalwareMustDie, malware)

http://securityaffairs.co/wordpress/53285/malware/malwaremustdie-closed.html