# New Indicators of Compromise for APT Group Nitro Uncovered

unit42.paloaltonetworks.com/new-indicators-compromise-apt-group-nitro-uncovered/

Jen Miller-Osborn October 3, 2014

By Jen Miller-Osborn

October 3, 2014 at 2:00 PM

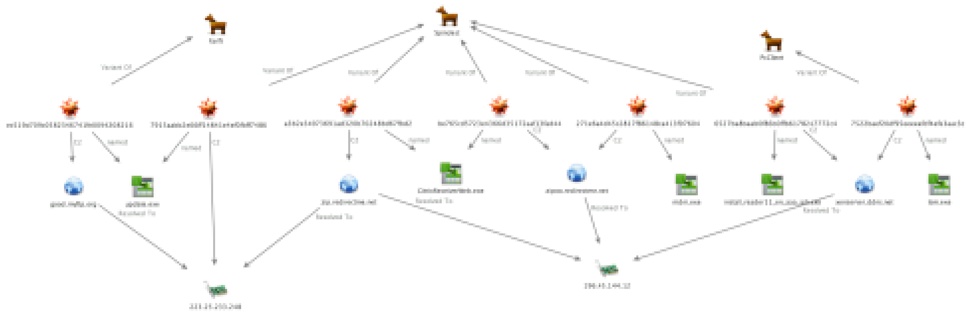
Category: Malware, Threat Prevention, Unit 42

Tags: APT, Nitro, URL filtering, WildFire

In mid-July of this year, we noticed yet another legitimate website had been compromised by APT actors and was serving malware. In this case, it was a group commonly referred to as "Nitro," which was coined by Symantec in its 2011 whitepaper.

As we dug deeper, we found additional compromised legitimate websites and malware from the same group back through March of this year. In most instances, the malware is one commonly referred to as "Spindest," though we also found "PCClient" and "Farfli" variants in use by the group. We don't have enough data to say for certain that all of the malware in this blog was delivered via compromised legitimate websites.

Historically, Nitro is known for targeted spear phishing campaigns and using Poison Ivy malware, which was not seen in these attacks.  Since at least 2013, Nitro appears to have somewhat modified their malware and delivery methods to include Spindest and legitimate compromised websites, as reported by Cyber Squared's TCIRT.  Our findings indicate they are continuing to evolve with the addition of PCClient and Farfli variants.  The Maltego screenshot below shows the activity we describe in this blog.



These events impacted at least the following industries, across four waves:

- A US based IT Solutions provider;
- The European office of a major, US based commercial vendor of space imagery and geospatial content;
- A European leader in power technologies and automation for utilities and industry;
- A US based provider of medical and dental imaging systems and IT solutions.

In July, Nitro compromised a South Korean clothing and accessories manufacturer's website to serve malware commonly referred to as "Spindest." Of all the samples we've tied to this activity so far noted in this blog, this is the only one configured to connect directly to an IP address for Command and Control (C2). This IP address has been in use by this group for some time, which is interesting since they have evolved other components of their kill chain over time to ensure malware delivery, but oddly not altered their C2 infrastructure. It is simple for companies to block any outbound traffic to this IP, which would negate the effort Nitro put into successfully delivering the malware.

37 AV vendors within VirusTotal properly identify it, and the PE timestamp shows the day before we saw it. In addition, the following three samples were found roughly a week apart from each other, possibly indicating the timing of the waves of activity.

**Table 1**

| | |
|---|---|
| **SHA256** | 0a1103bc90725d4665b932f88e81d39eafa5823b0de3ab146e2d4548b7da79a0 |
| **MD5** | 7915aabb2e66ff14841e4ef0fbff7486 |
| **File Name** | update.exe |
| **File Size** | 106496 |
| **First Seen** | 2014-07-24 11:54:02 |
| **C2 IP** | 223.25.233.248 |

The next sample we found is commonly known as PCClient, which is not malware previously tied to this group. We discovered this, and many of the following samples, through historic IP resolution overlap between the same domains alternately resolving to either the 223.25.233.248 or 196.45.144.12. The second IP has also not been reported as tied to this group before. However, this shifting of IP resolutions back and forth indicates Nitro is in control of these domains. It also makes is fairly easy for any Infosec team to reach the same conclusion we did, which again negates their use both of a previously unreported domain and IP for C2, as well as a new family of malware. 25 AV vendors within VirusTotal properly classify this sample as malware. Its PE timestamp was 8 July, almost a week prior when we first saw it.

**Table 2**

| | |
|---|---|
| **SHA256** | 8aef92a986568ba31729269efa31a2488f35920d136ab41cb6fce55fd8e0b4b7 |
| **MD5** | 7522baef20df95eeeeafdf4efe3aac3c |
| **File Name** | lsm.exe |
| **File Size** | 65536 |
| **First Seen** | 2014-07-15 11:48:33 |
| **C2 URL** | xenserver.ddns[.]net |
| **Resolution** | 196.45.144.12 |

The next sample was another Spindest variant and had the same timestamp as the aforementioned PcClient sample.  In addition, Nitro chose to use the same C2 for this sample, making it easy to both find and tie to the group. 41 AV vendors within VirusTotal properly classify this sample as malware.

**Table 3**

| | |
|---|---|
| **SHA256** | 995bc16a5c2c212b57ba00c2376ac57c8032c7f2b1d521f995a5e1d49066d64d |
| **MD5** | 6527ba8baab0f86b0ffb6178247772c4 |
| **File Name** | install_reader11_en_aaa_aih.exe |
| **File Type** | PE |
| **File Size** | 81920 |
| **First Seen** | 2014-07-09 16:31:26 |
| **C2 URL** | xenserver.ddns[.]net |
| **Resolution** | 196.45.144.12 |

The next wave of activity we found took place in mid-May. Both samples were Spindest variants with the same PE timestamp of 15 May. While neither MD5s for C2 match, the aforementioned link to a post by Cyber Squared's TCIRT did document Nitro using Spindest variants with the same file name starting late December last year. In that case they used the historic C2 IP we note in Table 1 in this blog. 34 AV vendors within VirusTotal properly classify the first sample as malware, and 40 AV Vendors the second sample.

**Table 4**

| | |
|---|---|
| **SHA256** | e7f2af8c48f837da57000c068368d77bc9b06eba1e077edfab58df6aa2ea40ec |
| **MD5** | 271e6a4d45c2817f86148ca413f97604 |
| **File Name** | mdm.exe |
| **File Size** | 118784 |
| **First Seen** | 2014-05-20 08:43:15 |
| **C2 URL** | zipoo.redirectme[.]net |
| **Resolution** | 196.45.144.12 |

**Table 5**

| | |
|---|---|
| **SHA256** | e601da16f923b33465dbafbff9d47195e8fc50099fd0581a16a1745bf890afb6 |
| **MD5** | be765cd5723e4366d35172aaf13fad44 |
| **File Name** | CitrixReceiverWeb.exe |
| **File Size** | 135168 |
| **First Seen** | 2014-05-15 16:34:10 |
| **C2 URL** | zipoo.redirectme[.]net |
| **Resolution** | 196.45.144.12 |

The malware dropped was configured to use good.myftp[.]org as the C2 URL, and the IP resolution was 223.25.233.248.  Both of these are known Nitro Indicators of Compromise (IOCs). In this case, the malware was a Farfli variant, again not a malware previously tied to this group. 39 AV vendors within VirusTotal properly identify the file as malware.  The PE timestamp on the file was 1 April, about two weeks before we saw the file. Continuing the activity, we discovered the actors had compromised a legitimate website belonging to an international technology company that provides Software Configuration and Change Management (SCCM) solutions in mid-May. (It is a well regarded company and partners with large companies such as Microsoft.)

**Table 6**

| | |
|---|---|
| **SHA256** | 184c083e839451c2ab0de7a89aa801dc0458e2bd1fe79e60f35c26d92a0dbf6a |
| **MD5** | ec519d709c0582346741fe0094208216 |
| **File Name** | update.exe |
| **File Size** | 159744 |

| | |
|---|---|
| **First Seen** | 2014-04-15 01:13:14 |
| **C2 URL** | good.myftp[.]org |
| **Resolution** | 223.25.233.248 |

The final sample, from mid-March, was also hosted on a compromised legitimate website, this time a small, US based IT company.  The IP resolved by the C2 URL was changed two days after we saw this file to overlap with good.myftp[.]org for a month before returning the below resolution. The filename matches that of the sample in Table 5, which had a very similar third level C2 domain and the same IP resolution. This is also a Spindest variant with a PE timestamp of the same day we saw it. 39 AV vendors within VirusTotal properly identify the file as malware.

**Table 7**

| | |
|---|---|
| **SHA256** | ffbddfb536e8e604c880ec977d06f804a500fc0396899bd2c195fb1f5b74207a |
| **MD5** | a3b2e34973691ad320b70248bd67fbd2 |
| **File Name** | CitrixReceiverWeb.exe |
| **File Size** | 192512 |
| **First Seen** | 2014-03-12 06:58:22 |
| **C2 URL** | zip.redirectme[.]net |
| **Resolution** | 196.45.144.12 |

As this post and previous cited research show, APT groups such as Nitro will continue to evolve their techniques within the kill chain to avoid detection.  However, they also demonstrate the value of tracking these threats over time, as this allowed us to uncover and properly attribute the new IOCs because Nitro was still re-using old C2 infrastructure with their new malware.

For Palo Alto Networks customers, all of these files were properly identified by WildFire as malware and all of the C2 domains are labeled as threats in both Threat Prevention and URL Filtering systems.