



# Sakula Reloaded

THE ADVERSARY LINE-UP • 18 NOV 2015 • MATT DAHL

Often during the investigation of sophisticated threat actors, the demarcation between the different attackers and campaigns are blurry. Researchers need to rely on tradecraft and analytic rigor to understand the unseen components of the attack, this often necessitates an intelligence assessment. The use of an intelligence assessment around a set of activity introduces room for error, which is generally balanced with confidences and likelihoods. A window into the mind of the analyst making these assessments and the difficulty imposed by the ambiguity of looking at the fragments of an attack can be glimpsed through the case of the malware dubbed Sakula.

Sakula is a well known malware variant linked to several significant targeted intrusion campaigns over the past 2-3 years. This remote access toolkit has been publicly examined multiple times by the threat intelligence community. CrowdStrike has released two blog posts detailing Sakula campaigns and continues to investigate its usage. In the past two years, two campaigns of Sakula activity stand out as being particularly significant – the [“French Aerospace” Campaign](#) and the [“Ironman” Campaign](#). In recent months, CrowdStrike has observed limited use of what appears to be a third Sakula variant.

Investigation into the use of Sakula malware leads the CrowdStrike analyst to assess that there is no definitive connection between these three campaigns. Further the analyst assesses that Sakula is a limited-release tool in use by multiple adversaries. An interesting facet of this malware to highlight, is the apparent connection between the use of Sakula and PlugX. In one case detailed below, Sakula was directly observed as a first stage used to deliver a second stage PlugX payload, and in another case there is evidence that Sakula and PlugX samples have relied on the same command and control (C2) infrastructure. What follows is a brief discussion of a recent Sakula campaign and a summary of previously observed Sakula activity.

## The INOCNATION Campaign

In early July, CrowdStrike’s Falcon Host technology detected an attack leveraging the CVE-2015-5119 exploit code that was publicly exposed after the breach of the European information security company Hacking Team. The exploit was hosted at [www\[.\]cbppnews\[.\]com/movie.swf](http://www[.]cbppnews[.]com/movie.swf), which CrowdStrike speculates was meant to spoof the website of the US-based think tank “Center on Budget and Policy Priorities”. Upon successful exploitation, a file was saved at “%Temp%/Rdws.exe” which is executed and writes another file at “%TEMP%/adobe.dat.” This file was used as a first stage downloader to retrieve a second stage PlugX file that connected to several C2 domains beginning with [cdn\[.\]sanecat\[.\]com](http://cdn[.]sanecat[.]com). Analysis of this first stage downloader revealed it to be a new variant of Sakula malware.

About a month later, in early August 2015, Falcon Host detected similar suspicious activity. The investigation of this activity identified malware included in a fake installer alleging to be a security plugin customized to the target organization. This attack was assessed to be part of highly tailored phishing campaign, which utilized a registered domain purporting to be owned by the target organization's security team. Once activated, the malware beaconed to port 443 on the same domain used to send the initial phishing email.

Finally, a few weeks after the second incident, CrowdStrike identified another sample of the new Sakula variant. This new file masqueraded as an installer for legitimate software and conducted C2 communications with the domain inocnation[.]com. This domain appears to be meant to spoof that of a legitimate entity which would indicate the target for this campaign, although it is unclear at this time exactly which organization this may be. Possible candidates for this targeting include the Iraq National Oil Company or the Indian National Overseas Congress.

### The Ironman Campaign

Before the identification of this new variant, CrowdStrike last publicly reported on Sakula in November 2014. That investigation began in late July 2014 when CrowdStrike identified an interesting file with zero anti-virus detections being used to drop an older variant of the Sakula malware. The file was an executable disguised as an installer for Adobe software signed with a certificate for the organization DTOPTOOLZ Co., Ltd. When opened, this file displayed a spoofed webpage for an American university alumni event and also dropped a Sakula payload that communicated with a C2 IP address of 180.210.206.246.

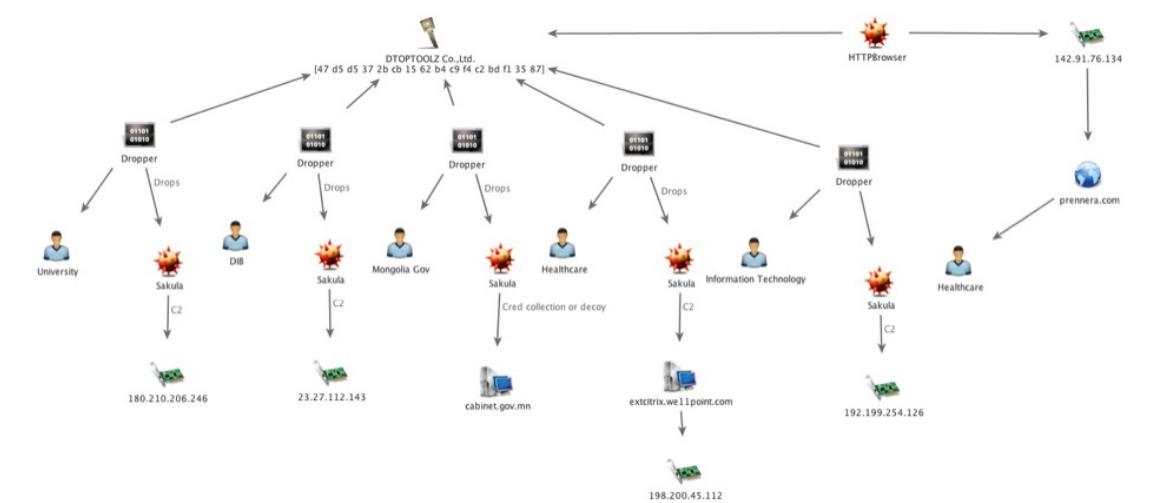
Within days of the discovery of this file, two other similar Sakula dropper files were identified that were also disguised as installers for legitimate software, redirected victims to sites meant to spoof the legitimate sites of the target organizations, and were also signed with the DTOPTOOLZ certificate. These incidents targeted a US-based defense company and the Mongolian government.

The use of a fake installers, spoofed domains, and Sakula malware overlaps the tactics, techniques, and procedures of the Ironman campaign with the activity observed during the INOCNATION Campaign. A table highlighting notable similarities between the Ironman and INOCNATION Campaigns follows.

CODE SIMILARITIES WITH OLDER SAKULA SAMPLES	TTP SIMILARITIES BETWEEN IRONMAN AND INOCNATION CAMPAIGNS	NOTABLE DIFFERENCES BETWEEN OLD AND NEW VARIANTS
C2 protocol with integer-based command ID	Malware disguised as an installer for legitimate software	Old variant communicates over plain HTTP; New variant over HTTPS
Same dropper used with previous Sakula activities	Malware leverages domain spoofing target entity	C2 message formats differ between old and new variants
Both variants likely use same build environment	Malware displays spoofed login page for target entity	

Further research revealed additional Sakula samples signed with the DTOPTOOLZ certificate□ dating back to April 2014 that appeared to be targeted at a healthcare organization and an IT business serving US government clients. One of these files communicated with the domain□ we11point[.]com domain which appeared to be a spoof of the website for the healthcare company, WellPoint, which is now known as Anthem. The spoofed domain suggests that the WellPoint healthcare organization was a target in this campaign, and, in fact, in February 2015, Anthem announced a massive data breach which is believed to be the result of a compromise by China-based targeted intrusion actors

The Anthem breach announcement preceded a number of similar notifications from other□ healthcare entities like Premera and CareFirst, and the U.S. government's Office of Personnel□ Management. Security researchers investigating this activity found additional indicators suggesting that the operators carrying out the DTOPTOOLZ Sakula campaign were the same ones responsible for all of these breaches.



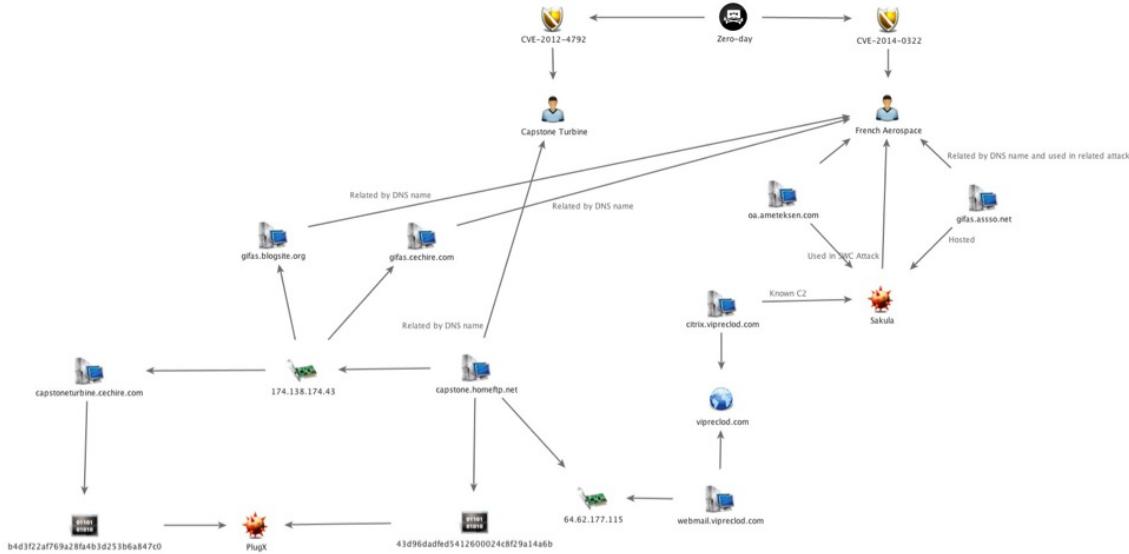
It should be noted that a previous blog post discussed possible connections between the Ironman Campaign and CrowdStrike's DEEP PANDA adversary. Further investigation into this campaign and Sakula activity in general has reduced confidence in this connection and it now appears□ unlikely that the two are linked.

### The French Aerospace Campaign

CrowdStrike's first public report on Sakula activity came in February 2014, as a result of strategic□ web compromise (SWC) activity affecting French aerospace-related websites. The SWC leveraged what was, at the time, zero-day exploit code for the CVE-2014-0322 vulnerability. The payload ultimately delivered in these attacks was Sakula connecting to a command and control (C2) domain of oa[.]ameteksen[.]com.

Some of the general Tactics, Techniques, and Procedures (TTPs) of this operation were shared with a 2012 SWC attack using the website of US-based turbine manufacturer Capstone Turbine to host a zero-day exploit. The tactical similarities include the use of SWC sites to infect victims, the use of exploit code for zero-day vulnerabilities, and overlaps in the infrastructure used. Specifically, the known Sakula C2 domain webmail[.]vipreclod[.]com has shared infrastructure□

with the Capstone Turbine-themed domain `capstone[.]homeftp[.]net`, suggesting that the same operators conducting the Capstone Turbine activity also used Sakula. This infrastructure has also been leveraged as C2 for PlugX samples. Furthermore, the Capstone Turbine-related infrastructure also includes multiple domains referencing “GIFAS” which is the acronym for the French Aerospace Industries Association (Groupement des industries françaises aéronautiques et spatiales). GIFAS-themed domains were also used in the February 2014 SWC activity.



## Conclusion

The Sakula malware demonstrates the difficulty of attribution and the rationale for bookending technical information with analytic judgements. Sakula has relatively restricted deployments when compared to more widespread RATs used by China-based adversaries such as PlugX. Its use is linked to the use of a number of zero-day exploits and high-profile incidents such as those resulting in the healthcare and government data breach notifications earlier this year. While its use is relatively limited, prolonged monitoring of Sakula activity leads the CrowdStrike Intelligence team to assess that it is likely used by a small subset of operators, which, given the access to zero-day exploits and high-profile operations, are likely well-resourced. □

For more information on the Sakula malware, feel free to contact us at [intelligence@crowdstrike.com](mailto:intelligence@crowdstrike.com). If you think you are up to the challenge of analyzing and investigating the motivations of malicious adversaries, check our [job listings](#) to join the mission!



Leave a Reply

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

Name \*

Email \*

Website

Comment

Post Comment

← Nothing else is working. Why not  
memory forensics?

7 Key Steps to Improve Your Network  
Defenses →



## Follow Us

### Tweets



 **George Kurtz**  
@George\_Kurtz

10h

Great Blog post from @CrowdStrike -> Sakula Reloaded  
[blog.crowdstrike.com/sakula-reload...](http://blog.crowdstrike.com/sakula-reload...)

Retweeted by CrowdStrike

Expand



 **George Kurtz**  
@George\_Kurtz

10h

Great Blog post from @CrowdStrike -> Sakula Reloaded  
[blog.crowdstrike.com/sakula-reload...](http://blog.crowdstrike.com/sakula-reload...)

Expand



 **adam\_cyber**  
@Adam\_Cyber

18h

Blog post on Sakula malware and its use delivering PlugX - also clarification on DeepPanda and Sakula: [blog.crowdstrike.com/sakula-reload...](http://blog.crowdstrike.com/sakula-reload...)

Expand



 **Steven Chabinsky**  
@StevenChabinsky

20h

G20 nations, including China, agree not to conduct or support online theft of intellectual property/trade secrets. [thehill.com/policy/cyberse...](http://thehill.com/policy/cyberse...)

Show  
Summary



 **CrowdStrike**  
@CrowdStrike

17 Nov

Read about The 7 Key Steps to Improve Your Network Defenses on our Blog: [ow.ly/UL88v](http://ow.ly/UL88v)  
#cybersecurity #infosec #endpoint #security

Expand

Compose new Tweet...

## Recent Posts



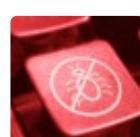
### The Imperative for Proactive Incident Response in 2015 and Beyond

November 3, 2015



### Why Your Business Environment Should Drive Cybersecurity

November 2, 2015



### Blurring of Commodity and Targeted Attack Malware

October 16, 2015



## Should I Really Trust the Cloud with my Endpoint Protection?

September 30, 2015



## U.S. – China Agreement on Cyber Intrusions: An Inflection Point

September 25, 2015

### Archives

							N	O	V	E	M	B	E	R	2	0	1	5
M	T	W	T	F	S	S												
															1			
<u>2</u>	<u>3</u>	4	5	6	7	8												
9	10	11	12	<u>13</u>	14	15												
16	17	<u>18</u>	19	20	21	22												
23	24	25	26	27	28	29												
30																		

« Oct

### Recent Comments