DEEP PANDA Uses Sakula Malware to Target Organizations

crowdstrike.com/blog/ironman-deep-panda-uses-sakula-malware-target-organizations-multiple-sectors/

November 24, 2014

I am Ironman: DEEP PANDA Uses Sakula Malware to Target Organizations in Multiple Sectors

November 24, 2014

Matt Dahl Research & Threat Intel

Over the last few months, the CrowdStrike Intelligence team has been tracking a campaign of highly targeted events focused on entities in the U.S. Defense Industrial Base (DIB), healthcare, government, and technology sectors. This campaign infected victims with *Sakula* malware variants that were signed with stolen certificates. Investigation into this activity led to associations with the adversary known to CrowdStrike as DEEP PANDA.

On 31 July 2014, an executable was identified, which, at the time, was not detected by any anti-virus products. When this file was executed, it caused the victim to view a website by using the ShellExecute() API to open a URL. The site's domain name was meant to spoof that of a site set up to provide information on an alumni event for a U.S university. This page requested that the visitor download an Adobe-related plugin in order to view the content. The downloaded plugin file included a variant of Sakula malware. [1]

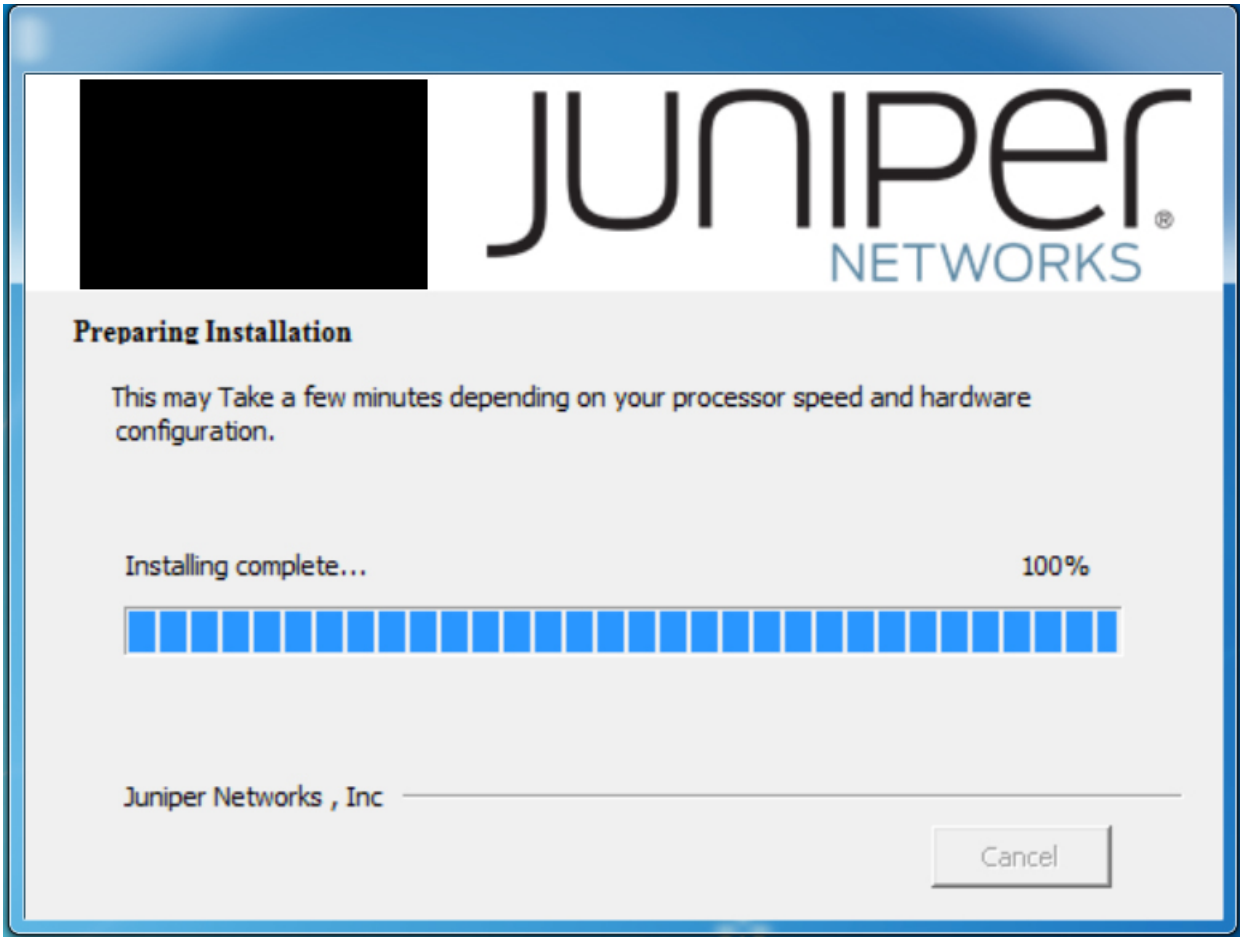
The Sakula malware in this campaign utilized the Dynamic Link Library (DLL) side-loading technique most commonly associated with *PlugX* activity. In the aforementioned university-related incidents, a legitimate executable named MediaSoft.exe (MD5 hash: d00b3169f45e74bb22a1cd684341b14a) loaded a file named msi.dll (MD5 hash: ae6f33f6cdc25dc4bda24b2bccff79fe), which, in turn, was used to load the Sakula executable (MD5 hash: 0c2674c3a97c53082187d930efb645c2). This final executable was also signed with a certificate assigned to an organization called DTOPTOOLZ Co., Ltd.

Command-and-Control (C2) communications in this incident went directly to IP address 180.210.206.246; a sample GET request is below:

```
GET /photo/fxwcac1331366747.jpg?id=232304 HTTP/1.1
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; WOW64;
Trident/4.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR
3.0.30729; Media Center PC 6.0)
Host: 180.210.206.246
Cache-Control: no-cache
Cookie: ASPSESSIONIDSATCSBAQ=CHPHOJEBGCLJBBPGBEGNOHPA
```

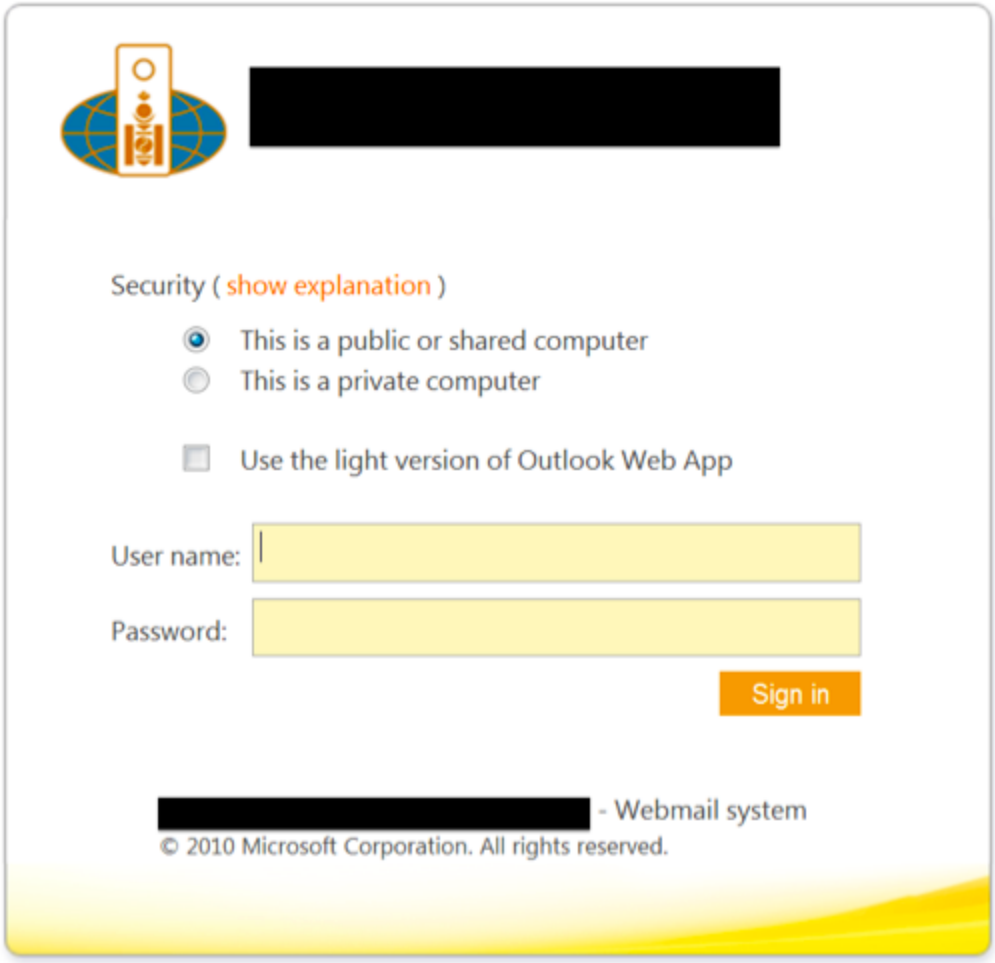
Further investigation revealed similar activity stretching back to at least April 2014, when similar TTPs were used to target a healthcare organization and a U.S.-based IT company with high-profile clients in the defense sector. Two other incidents were also identified in August 2014 targeting a company in the DIB and a Mongolian government entity.

All incidents in this campaign were similar in that they utilized malicious droppers masquerading as installers for legitimate software applications like Adobe Reader, Juniper VPN, and Microsoft ActiveX Control. They display progress bars that make it appear as if the specified software is being updated or installed.



Example of Installer Progress Bar Displayed by Dropper

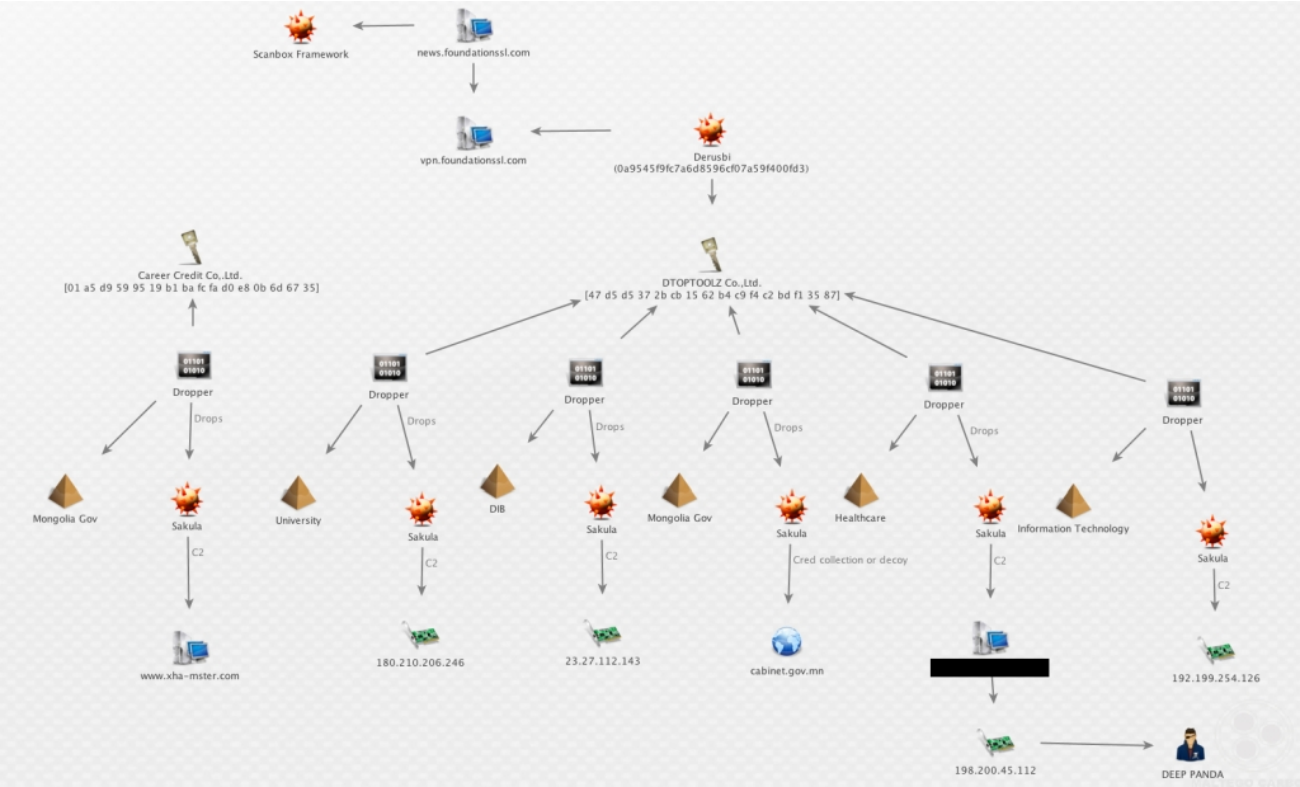
In addition, the droppers all directed victims to login pages for services specific to the target organization like webmail, document sharing, or corporate VPN. In all cases except one, the victims were directed to legitimate login pages. The one exception was a case in which victims were sent to a login page hosted on a domain that spoofed that of the legitimate one. It is unclear whether redirecting victims to these login pages was part of credential-collection activity or merely meant to deceive victims into believing that the activity was legitimate.



Example of a Login Page that Victims were Redirected to

The campaign appeared to be over by the end of August, but a file was recently discovered that suggests it may be ongoing. The intended target again appeared to be a Mongolian government entity, and the file masqueraded as an installer for Microsoft ActiveX software. It dropped the side-loaded Sakula malware just like in the other incidents; however, in this instance, the Sakula payload was signed with a certificate assigned to a different organization, Career Credit Co., Ltd. The malware used the domain *www[.]xha-mster[.]com* for C2 which was created in mid-September and is registered with the email address wendellom@yahoo.com and registrant name “tonyy starke” (hence the name, Ironman-related title for this blog).

Below is a chart showing the relevant relationships to this DEEP PANDA campaign.



The bottom of the chart shows an infrastructure connection between an IP address (198.200.45.112) used this campaign and also used in recently observed DEEP PANDA activity.

Association with Recent Scanbox Activity

In September 2014, CrowdStrike Intelligence identified a malicious file signed with the DTOPTOOLZ Co., Ltd. certificate. Analysis of this file revealed it to be Derusbi malware (a favorite RAT of DEEP PANDA) that used the domain *vpn[.]foundationssl[.]com* for its C2. At the time of discovery, CrowdStrike did not attribute the file to DEEP PANDA based on the malware alone, but the use of the DTOPTOOLZ certificate to sign a malware variant known to be heavily used by this adversary makes it likely that this signed Derusbi sample is also attributable to DEEP PANDA.

In a recent public report from PWC, another *foundationssl[.]com* domain was linked to activity involving the Strategic Web Compromise (SWC) framework more commonly known as Scanbox. In that operation, the Scanbox code was placed on the website of a U.S.-based think tank and utilized the malicious domain, *news[.]foundationssl[.]com*. The use of the two *foundationssl[.]com* subdomains suggests that the same adversary (in this case DEEP PANDA) was responsible for the signed Derusbi malware file and the think tank SWC activity. Furthermore, CrowdStrike publicly reported on DEEP PANDA targeting of think tanks in July 2014.

If you want to hear more about DEEP PANDA and their tradecraft or any of the other adversaries that CrowdStrike tracks, please contact: sales@crowdstrike.com

[1] In February 2014, CrowdStrike publicly reported on a campaign that leveraged Sakula malware (http://www.crowdstrike.com/blog/french-connection-french-aerospace-focused-cve-2014-0322-attack-shares-similarities-2012/index.html); however, the Tactics, Techniques, and Procedures (TTPs) between that campaign and this recent one are different, suggesting two distinct adversaries are using the Sakula malware.

Who is EMBER BEAR?

A Tale of Two Cookies: How to Pwn2Own the Cisco RV340 Router

PROPHET SPIDER Exploits Citrix ShareFile Remote Code Execution Vulnerability CVE-2021-22941 to Deliver Webshell