New Disdain Exploit Kit Detected in the Wild

- Posted on:August 17, 2017 at 12:38 am
- Posted in:Exploits
- Author:
  Trend Micro

0

By Chaoying Liu and Joseph C. Chen

The exploit kit landscape has been rocky since 2016, and we've observed several of the major players—Angler, Nuclear, Neutrino, Sundown—take a dip in operations or go private. New kits have popped up sporadically since

then, sometimes revamped from old sources, but none have really gained traction. Despite that fact, cybercriminals continue to develop more of them.

On August 9, we detected a new exploit kit in the wild, being distributed through a malvertising campaign. With additional analysis of the code and activity, we can confirm that it is the Disdain exploit kit, which started to advertise their services in underground forums starting August 8. We found the "disdain" keyword contained in its JavaScript code.

We detected two different malvertising groups trying to use the new exploit service to deliver malware. One of the groups we were monitoring used Disdain to deliver the Smoke Loader Trojan (detected by Trend Micro as TROJ_SHARIK.VDA), which would then install a cryptocurrency miner.

Activity and analysis of Disdain

While we were tracking the exploit kit, we noted erratic activity that dipped on August 11 before quickly spiking on August 12. The activity dropped again after that. So far, since it is the early stages of the kit, detections have been minimal.

Disdain shares the same URL pattern as the Terror exploit kit, which is not the first time a new kit has borrowed from Terror. However, its JavaScript obfuscation style is similar to the Nebula exploit kit. The kit relies on older exploits (one is from 2013) as well as newer exploits, though all have been patched.

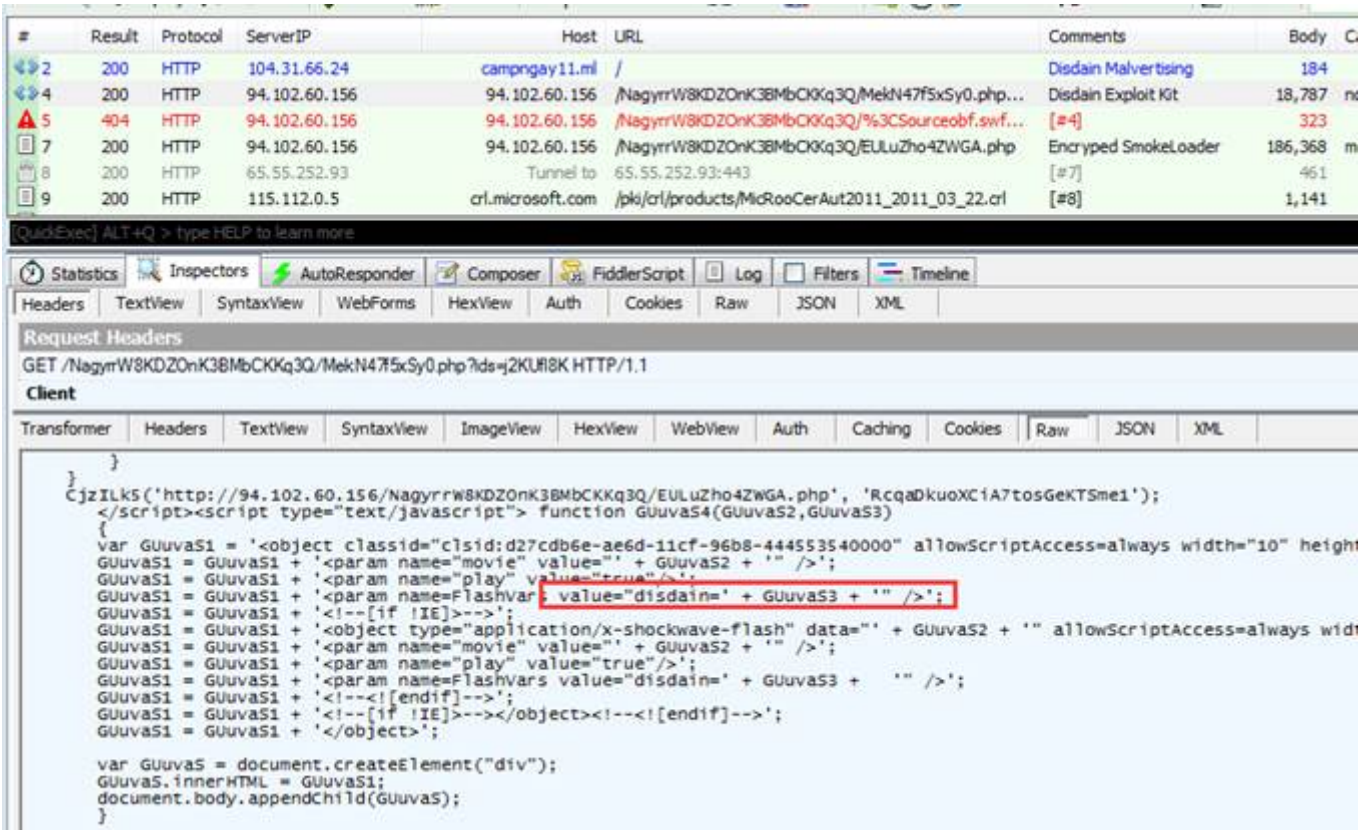


Figure 1. Keyword "disdain" contained in the exploit kit, seen delivering Smoke Loader

It seems that even in the underground, advertisements promise more than what the product can deliver. In their post on an underground forum, the developers listed 17 different CVEs that the kit currently exploits, but we observed only five:

- CVE-2013-2551, patched in May 2013
- CVE-2015-2419, patched in July 2015
- CVE-2016-0189, patched in May 2016

- CVE-2017-0037, patched in March 2017
- CVE-2017-0059, patched in March 2017

It's worth noting that the exploit kit combines CVE-2017-0059 and CVE-2017-0037 (the youngest CVEs) to exploit the IE browser. These exploits were first found in the wild: CVE-2017-0059 is an information disclosure vulnerability in IE that was patched on March 2017. With this CVE, the attacker gets the base address of propsys.dll and then evades Address Space Layout Randomization (ASLR), which is used to prevent exploitation of memory corruption vulnerabilities. CVE-2017-0037 is a type corruption vulnerability in IE and Edge, and the attacker uses it to execute shellcode. Used in tandem, these vulnerabilities would allow the attacker to execute arbitrary code on a compromised device.

However, the related malicious code can't actually exploit anything because of certain faults by the developer.

```
var mMbRPJm18 = "";

function mMbRPJ3() {
    var textarea = document.getElementById("mMbRPJ5");
    var mMbRPJ141 = document.createElement("iframe");
    textarea.appendChild(mMbRPJ141);
    mMbRPJ141.contentDocument.onreadystatechange = mMbRPJ367;
    mMbRPJM44.reset();
}

function mMbRPJ367() {
    document.getElementById("mMbRPJ5").defaultValue = "foo";
    var mMbRPJ60 = document.createElement("audio");
    mMbRPJ60.src = "test.mp3";
}
```

Figure 2. Code fragment of CVE-2017-0059

```
<style>
    .mMbRPJ1 {
        float: left;
        column-count: 5;
    }

    .mMbRPJ2 {
        column-span: all;
        columns: 1px;
    }

    table {
        border-spacing: 0px;
    }
</style>
<script type="text/javascript">
    <!--
    function mMbRPJ100() {
        document.styleSheets[0].media.mediaText = "aaaaaaaaaaaaaaaaaaa";
        mMbRPJm40.align = "right";
    }
    setTimeout(function() {
        var ABmMbRPJ = document.getElementById("mMbRPJ5");
        var mMbRPJm32 = ABmMbRPJ.text.substring(0, 2);
        var mMbRPJm29 = mMbRPJm5(mMbRPJm32);
        mMbRPJm18 = mMbRPJm29 - 0xbacc;
        mMbRPJm18 = mMbRPJm18.toString(16);
        mMbRPJ101();
        mMbRPJ100();
```

Figure 3. Code fragment of CVE-2017-0037

Solutions and recommendations

All the listed CVEs that Disdain exploits have been patched, some even years before the kit was detected. This only emphasizes the need for timely patching—enterprises and users alike should prioritize critical patches and be diligent in protecting their system from preventable compromises.

Aside from patching, a multilayered approach to security is also necessary to defend against complex threats. A comprehensive solution covers all flanks—from the gateway, endpoints, networks, and servers. 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's endpoint solutions such as 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.

Hat tip to ProofPoint's kafeine whom we worked with on this research.

Indicators of Compromise

www[.]hidretds[.]com	Malvertising domain
campngay11[.]ml	Malvertising domain
campngay11[.]gq	Malvertising domain
campngay12[.]gq	Malvertising domain
94[.]102[.]60[.]156	Disdain exploit kit IP address
a11t01t22t10[.]ru	Smoke Loader C&C domain
789e26249acaa412d1ea58fff45927d722ab4badb69c0c90ad0efc9cc0541d3e	Smoke Loader
9fdbcc58d935baebf473c4ab30c47df9d91414423e2fa5dc3b38c7757f175bd1	Cryptocurrency miner

Related Posts:

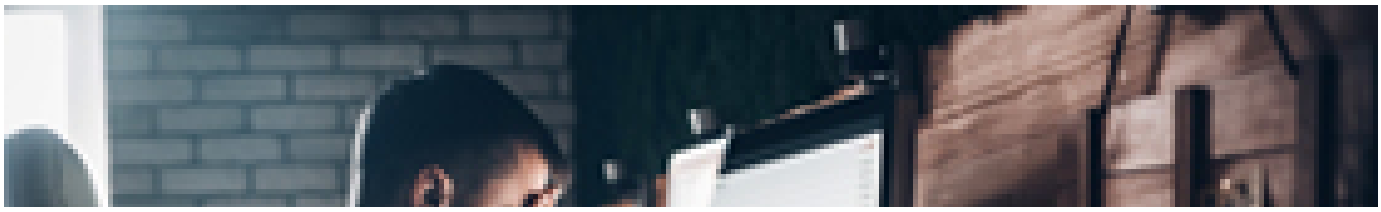
- **Will Astrum Fill the Vacuum in the Exploit Kit Landscape?**
- **One Bit To Rule A System: Analyzing CVE-2016-7255 Exploit In The Wild**
- **ProMediads Malvertising and Sundown-Pirate Exploit Kit Combo Drops Ransomware and Info Stealer**
- **Updated Sundown Exploit Kit Uses Steganography**

Tags: exploit kit

Featured Stories

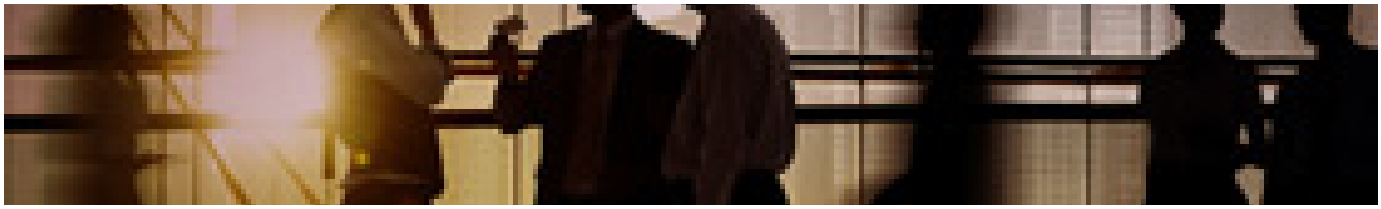
- Following the Trail of BlackTech's Cyber Espionage Campaigns
- Android Backdoor GhostCtrl can Silently Record Your Audio, Video, and More
- Linux Users Urged to Update as a New Threat Exploits SambaCry
- Erebus Resurfaces as Linux Ransomware
- The Reigning King of IP Camera Botnets and its Challengers

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.

Business Email Compromise



- How can a sophisticated email scam cause more than $2.3 billion in damages to businesses around the world?
  See the numbers behind BEC

Latest Ransomware Posts

Cerber Ransomware Evolves Again, Now Steals From Bitcoin Wallets

New WannaCry-Mimicking SLocker Abuses QQ Services

LeakerLocker Mobile Ransomware Threatens to Expose User Information

SLocker Mobile Ransomware Starts Mimicking WannaCry

Large-Scale Petya Ransomware Attack In Progress, Hits Europe Hard

Recent Posts

- New Disdain Exploit Kit Detected in the Wild
- GhostClicker Adware is a Phantomlike Android Click Fraud
- The Crisis of Connected Cars: When Vulnerabilities Affect the CAN Standard
- CVE-2017-0199: New Malware Abuses PowerPoint Slide Show
- Can Online Dating Apps be Used to Target Your Company?

Ransomware 101

- 

This infographic shows how ransomware has evolved, how big the problem has become, and ways to avoid being a ransomware victim.
Check the infographic

Popular Posts

The Crisis of Connected Cars: When Vulnerabilities Affect the CAN Standard
CVE-2017-0199: New Malware Abuses PowerPoint Slide Show
A Look at JS_POWMET, a Completely Fileless Malware
Android Backdoor GhostCtrl can Silently Record Your Audio, Video, and More
Linux Users Urged to Update as a New Threat Exploits SambaCry

Latest Tweets

- The #Disdain #exploitkit delivers the Smoke Loader Trojan, which would then install a cryptocurrency miner. Details: bit.ly/2x8SaJv
  about 1 hour ago
- #Ransomware capitalizes on fear. Take their leverage away by following these preventive measures:… twitter.com/i/web/status/8…
  about 7 hours ago
- The #carhack we recently discovered is currently undetectable and indefensible by current security measures.Details… twitter.com/i/web/status/8…
  about 1 day ago

Stay Updated

Email Subscription

Your email here

Subscribe