CYBERCRIMINALS INTEGRATE EXPLOIT FOR CVE-2018-8174 INTO NUMEROUS ATTACK TOOLS

By Verint Cyber Threat Intelligence Research Team July 18, 2018

Share this Article

The CVE-2018-8174 vulnerability in Internet Explorer was found using OSINT tools and used by a nation-state group from North Korea. By constantly monitoring news outlets with WEBINT platforms, we discovered that the vulnerability was later adopted by cyber criminals globally, and was embedded inside exploit kits that were traded throughout dark-web platforms. The following is an in-depth exploration of our findings surrounding the vulnerability.

The CVE-2018-8174 vulnerability, also dubbed "Double Kill," was discovered in the beginning of May 2018, when it was exploited as a 0-day in an APT attack leveraging malicious Office files in China. The vulnerability affects users with Internet Explorer installed, either after they browse the web or after they open crafted Office documents – **even if the default browser on the victim's machine is not set to IE. Moreover, it also affects IE11, even though VBScript is no longer supported by using the compatibility tag for IE10.** Microsoft patched the vulnerability on May 8, 2018.

We use WEBINT tools frequently to monitor underground hacking communities, in this case, our monitoring revealed that since its discovery, various threat actors in the Russian underground hacking scene have shown a keen interest in this particular vulnerability, indicating their strong intent to exploit it in attacks. Since then, **we have observed exploits for this vulnerability incorporated into several prominent attack tools used by Russian threat actors, including the *RIG Exploit Kit* and the *Threadkit* package of Office exploits indicating that cybercriminals see it as a profitable attack vector**. Concurrently, security reports state that the exploitation of this vulnerability has been witnessed in additional attack campaigns.

THE CVE-2018-8174 EXPLOIT

The vulnerability exists in the VBScript – incorporated both in the Internet Explorer browser and in Microsoft Office software. Being a use-after-free (UAF) memory vulnerability, it is particularly dangerous because of the enabling of the execution of arbitrary code, or, in some cases, full remote code execution, due to access to read and write primitives.

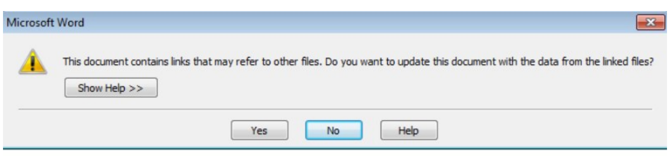
The APT attack spotted in China, later attributed to North Korean threat actors, used the URL Moniker technique to load the VisualBasic exploit leveraging CVE-2017-8174 into the Office process. Unlike previously-known Office exploits that used the same technique, the URL link in the current exploit calls the *mshtml.dll*, which is a library that contains the Visual Basic engine in Internet Explorer. **Thus, albeit delivered via a Word document as the initial attack vector, the exploit takes advantage of a vulnerability in VBScript, and not in Microsoft Word.**

This attack vector allows the attackers to incorporate Internet Explorer Browser exploits directly into Office documents, enabling them to use it via spear-phishing and drive-by campaigns. Immediately upon its discovery, it was estimated that the vulnerability would be exploited in multiple attack campaigns in the near future.

The in-the wild exploit consisted of three stages:

- Delivery of a malicious Word document
- Once opened, an HTML page containing a VBScript code is downloaded to the victim's machine
- A UAF vulnerability is triggered, and shellcode is executed

Figure 1: *Microsoft Office alert pops-up when opening the crafted document*



Microsoft Word

This document contains links that may refer to other files. Do you want to update this document with the data from the linked files?

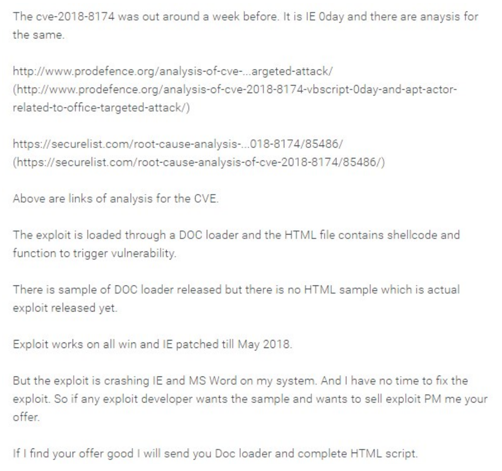
Download the eBook: Top 10 CTI Use Cases

UNDERGROUND CHATTER REGARDING THE EXPLOIT

> In less than two weeks, the exploit for CVE-2018-8174 was incorporated into the Metasploit framework
>
> CLICK TO TWEET

. At the same time, we have spotted vigorous chatter regarding this vulnerability emerging on underground sources, in particular in Russian-speaking forums. Threat actors sought to purchase the exploit, and others shared PoC samples for the explicit purpose of their analysis and further modification.

Figure 2: *CVE-2018-8174 exploit is mentioned on underground chatter. Source: Verint DarkAlert*



The cve-2018-8174 was out around a week before. It is IE 0day and there are anaysis for the same.

http://www.prodefence.org/analysis-of-cve-...argeted-attack/ (http://www.prodefence.org/analysis-of-cve-2018-8174-vbscript-0day-and-apt-actor-related-to-office-targeted-attack/)

https://securelist.com/root-cause-analysis-...018-8174/85486/ (https://securelist.com/root-cause-analysis-of-cve-2018-8174/85486/)

Above are links of analysis for the CVE.

The exploit is loaded through a DOC loader and the HTML file contains shellcode and function to trigger vulnerability.

There is sample of DOC loader released but there is no HTML sample which is actual exploit released yet.

Exploit works on all win and IE patched till May 2018.

But the exploit is crashing IE and MS Word on my system. And I have no time to fix the exploit. So if any exploit developer wants the sample and wants to sell exploit PM me your offer.

If I find your offer good I will send you Doc loader and complete HTML script.

Moreover, and in accordance with predictions made by security researchers, **exploitation of this vulnerability was included in some of the most popular attack tools on the Russian underground.** Of note, operators of malware targeting both Microsoft Office and IE browser announced the addition of the exploit to their attack tools, indicating that the malicious payload is to be delivered by one of these two vulnerable software types. As explained above,

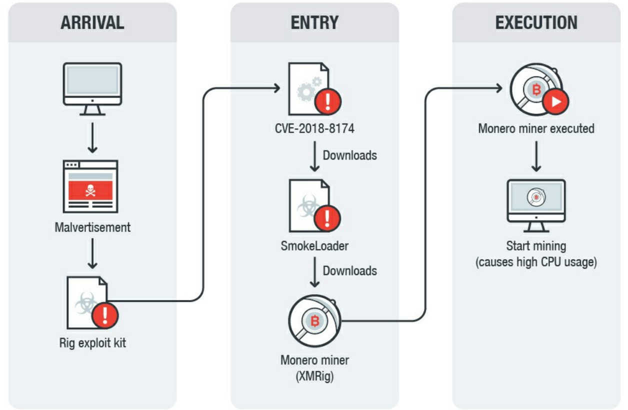
> the attack vector can be a malicious Microsoft Office file that will trigger the launch of IE browser, even if not configured as the default browser, or a crafted URL link directly provided to the target.
>
> CLICK TO TWEET

We detected an exploit for CVE-2018-8174 added to the following attack tools traded on the Russian underground:

- **The RIG exploit kit**[1] – in the wild attacks using this exploit to deliver the *Monero Miner* were already spotted.

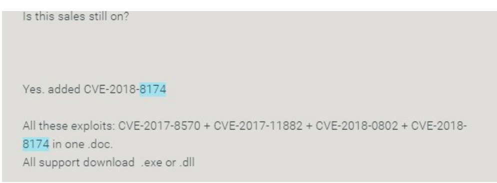
Read the ebook on the top 10 Cyber Threat Intelligence use cases that provide the visibility and proximity required for building a successful, proactive cyber threat intelligence operation.

Figure 3: The *RIG campaign's infection chain. Source: Trend Micro*



- **The Threadkit Office exploits package** – the modified version that includes the CVE-2018-8174 exploit is yet to be discovered in the wild. However, the malware's author already announced its incorporation several days ago. The update for the kit will cost US$ 400.
- **Another Office exploits package** – the new version includes exploits for the following vulnerabilities: CVE-2018-8174, CVE-2018-0802, CVE-2017-11882 and CVE-2017-8570.

Figure 4: Exploit *for CVE-2018-8174 is added to another office exploitation package. Source: Verint Dark Alert*



Is this sales still on?

Yes. added CVE-2018-8174

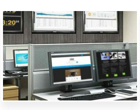
All these exploits: CVE-2017-8570 + CVE-2017-11882 + CVE-2018-0802 + CVE-2018-8174 in one .doc.
All support download .exe or .dll

AUTHOR: VERINT CYBER THREAT INTELLIGENCE RESEARCH TEAM
Verint's Cyber Threat Intelligence (CTI) research team (formerly SenseCy) is comprised of handpicked expert analysts, many of whom are ex-military intelligence, with years of experience in cyber threat intelligence and analysis. Our research team monitors, analyzes and validates threat actors' malicious activities on platforms such as social networks, mobile applications, Deep Web sites, Dark Web marketplaces, hacker forums, IRC channels, global CVEs and external threat intelligence generated by leading security providers. The Research team regularly produces threat alerts and intelligence reports based on region, industry and organization-specific threats, including in-depth analysis, actionable recommendations, IoCs and more, to proactively identify and mitigate threats before they materialize, to enhance resilience and prevent future attacks

MOST POPULAR:

Suspicious Domains Selling Tickets to the Tokyo 2020 Olympics

How Automation Turns CTI Analysts Into Super Heroes



Is a SIEM Enough to Make a SOC? Six Key Requirements for a Successful Security Operations Center

Trends in Terror. Is there any good news?

LET'S EMPOWER INTELLIGENCE

Contact Us

Products
Network Intelligence
Web & Social Intelligence
Tactical Intelligence
Intelligence Fusion
Cyber Security
Situational Intelligence
Video & Security

Solutions by Industry
National Security
Critical Infrastructure
Law Enforcement
Enterprise
National Intelligence
Transportation
Municipalities
Telecommunications Providers

Solutions by Security Challenge
Illegal Immigration
Regulatory Compliance & Audits
Terrorism
Cyber Threats
Drug Trafficking
Poaching
Human Trafficking
Theft & Vandalism
Financial Crime
Employee Safety
Active Shooter & Workplace Violence
Business Continuity
Natural Disasters
Facility & Asset Protection

Services
Open Source & Fusion Intelligence
Cyber Security
Situational Intelligence, Video & Security

Company
About
News
R&D Centers
Events
Resources
Blog
Contact Us

Partners
Cyber Intelligence
Cyber Security
Situational Intelligence, Video & Security

Careers

Contact Us

www.verint.com