CVE 2018-8453
MONTHLY RISK & THREAT ANALYSIS REPORT
PRODUCED DECEMBER 2018
THREAT ANALYSIS AND INVESTIGATIONS
Executive Summary

On December 6, 2018, threat actor X advertised the sale of the CVE-2018-8453 one-day exploit in a cyber crime forum. The exploit enables privilege escalation for an attacker that facilitates the full compromise of a victimized system. There is limited information on X, though he is associated with the sale of one-day exploits and enjoys a favorable reputation level, bolstering his bona fides as a reliable seller of merchandise. To date, suspected state actors have been observed leveraging the CVE-2018-8453 exploit against targeted entities in the Middle East region; however, the publicity surrounding this vulnerability coupled with slow implementation of available patches make any organization susceptible to compromise. Patch management remains a challenge for organizations and is necessary to reduce mitigation and remediation expenses incurred by companies post-compromise, which can be extremely costly.

Key Points

- In early December 2018, threat actor X advertised the sale of a one-day local privilege escalation exploit in a cyber crime forum. Elevation privilege exploits enable attackers to fully-compromise a victimized machine. Since its disclosure, hostile actors have been observed leveraging the CVE-2018-8453 exploit in targeted attacks directed against entities in the Middle East region.

- There is limited information on X. However, the actor is associated with advertising the sale of one-day exploits in the cyber crime underground in the past. Solid reputation levels and positive feedback from forum members indicate that the actor is a credible source of these types of exploits.

- Zero- and one-day vulnerabilities are generally considered critical for organizations to patch. While considered “rare” and typically believed to be used primarily by state actors, they nevertheless can be extremely costly for organizations to mitigate and remediate if they fail to promptly patch these vulnerabilities.

*This report is based on open source findings. Therefore, the report is open source intelligence and does not constitute definitive evidence. Information found in the open source cannot necessarily be verified and is presented as intelligence and as additional information to enhance or expand current investigations.*

*****
On December 6, 2018, Russian threat actor X advertised the sale of a one-day local privilege escalation (LPE) exploit CVE-2018-8453 for Windows operating systems in the Exploit[in] cyber crime forum (see Figure 1). The exploit enables an attacker to bypass Supervisor Mode Access Prevention (SMAP), kernel data execution prevention (DEP), kernel address space layout randomization (KASLR), Windows Integrity Level, and the user access control.

Per the actor’s posting, details of the exploit are as follows:


**Supported architecture:** x86 / x64

**Development stage:** v1.0.81207 (stable)

**x86 shellcode size:** 13Kb (avg. exec. time: 2-5 seconds)
The actor asserted that the code was written “from scratch.” Per X, the exploit comes in the form of shellcode (note: shellcode is instructions that go into effect once the code is deployed into an application), which is ready to be embedded into the attacker’s projects. At this time, a new function appears in the code:

```c
<BOOL GetSystemPWNED (ULONG ulProcessId);>
```

The actor states that the package contains demo source code that opens the command console with SYSTEM rights. For those potential buyers that work on bootkits/rootkitslockers, X asserts that the code can run in ring0 mode with some modifications (note: ring0 is the level with the most privileges and interacts with the computer’s hardware and memory). The actor claims that the exploit has been successfully tested on Windows builds ranging from XP SP0 to Windows 10 RS3 (approximately a hundred systems) from various years up through September 2018. The exploit is able to work under a “Guest” account, as well as from “Low Integrity” (note: the Windows Integrity Mechanism “provides the ability for resource managers, such as the file system, to use pre-defined policies that block processes of lower integrity from reading or modifying objects of higher integrity”). Additionally, the actor states that the exploit was tested on such security solutions as Kaspersky Total Security 2019, Avast Internet Security 2019, and ESET Smart Security 11. The actor indicates that other checks on security solutions are available on request.

The price of the exploit is listed at USD 10,000, payable in Bitcoin.

**What is CVE-2018-8453?**


An attacker who successfully exploited this vulnerability could run arbitrary code in kernel mode. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. To exploit this vulnerability, an attacker would first have to log on to the system. An attacker could then run a specially-crafted application that could exploit the vulnerability and take control of an affected system. In October 2018, Microsoft released a patch for this vulnerability.
Who is X?

Unsurprisingly, there is a dearth of information on the actor. The alias “X” is not unique in the cyber criminal underground, which makes it challenging to link the actor via this alias to specific postings. The actor’s postings in the underground have primarily focused on the sale of one-day exploits. Based on his favorability rankings, X provides valid exploits. The fact that the actor primarily operates in one cyber crime forum (at least under this alias) may be an attempt to reduce his footprint in the cyber crime underground and evade scrutiny from law enforcement elements.

Another alias associated with this actor is “Z”. This determination was made by linking the actor’s Jabber account playbit[@]exploit[.]im with a profile with that alias and a posting that he made on CVE-2016-7255. However, LookingGlass analysts believe that the actor solely uses the X alias on underground forums and Z as an alias for video sites such as YouTube and De-visions.

Cyber Crime Forums

Exploit[.]in. The actor joined this forum under the alias X on May 25, 2008. As of this writing, the actor has made approximately 90 posts, most of which focus on the sale of exploits and droppers. The actor enjoys a +10-favorability rating, which indicates that X has sold reliably in the past. Since June 24, 2012, the actor has opened threads that focused on selling one-day exploits for Windows OS. All feedback has been favorable.

Antichat[.]ru. The actor joined this forum under the alias X on May 20, 2012. The actor has only made one posting thus far in which he posted negative feedback about the sale of a dedicated server. The actor’s last visit on this site was on June 13, 2013.

Contact Information

Jabber

xyz[@]exploit[.]im

xyz[@]hacklab[.]li

Zero- and One-Day Exploits

Zero-day and one-day exploits refer to the amount of time that a company is aware of the vulnerabilities in their networks that could be taken advantage of by hostile actors. While zero-days refer to “holes” that an organization is not cognizant of (one academic paper on zero-days indicates that some of these exploits have gone unnoticed and unpatched for up to 10 months), one-days refer to an organization’s acknowledgement of a vulnerability.
that still remains unpatched. Zero-days are considered generally “rare”; the overwhelming majority of exploits faced by organizations are based on vulnerabilities generally known for approximately one year.\textsuperscript{v}

According to a first quarter 2018 report, a computer security company’s research found that zero-day markets are growing and maturing for anyone able to purchase them for legitimate or illegitimate reasons.\textsuperscript{vi} Per the same report, as of the first quarter in 2018, 45 zero-day vulnerabilities had been discovered (note: other vendors may have different statistics). Per a July 2018 Massachusetts Institute of Technology paper, an online subscription service offers zero-day exploits at a cost of approximately USD 150,000/month.\textsuperscript{vii} One company has found that zero-day attacks are increasingly being used by hostile actors to attack hybrid cloud environments.\textsuperscript{viii} Remediating the results of zero-day attacks can be costly for organizations. According to an online computer security news site, “the average company endures a cost of USD 7.12 million, or USD 440 per endpoint.\textsuperscript{ix}

**Patch Management is Important**

In an environment where attackers typically outpace the ability of network defenders, the ability to detect and patch vulnerabilities is critical for maintaining the confidentiality, integrity, and availability of information systems and the data resident on them. According to a company that specializes in a next-gen cloud Web Application Firewall that enables web applications to defend themselves, it takes more than a month for an “average organization” to patch its most critical vulnerabilities (like the one represented by the CVE-2018-8453 vulnerability).\textsuperscript{x} This is of paramount concern given that exploiting known vulnerabilities is a popular method for hostile actors to gain unauthorized access into organizations. According to a study by the Ponemon Institute that interviewed 3,000 worldwide cybersecurity professionals, more than half of breached organizations discovered that what facilitated the intrusion was the exploitation of a vulnerability for which a patch was available but had not been applied.\textsuperscript{xi} In 2017, 300 polled organizations of various sizes found that 80 percent of breaches were the result of poor patch management practices, according to a global analytic firm study.\textsuperscript{xii} When viewing the Equifax breach via the prism of an unpatched vulnerability, it is easy to see the potential dangerous fallout that can result.\textsuperscript{xiii}

Organizations are responsible for promptly patching vulnerabilities, especially those deemed high or critical risk by the National Institute of Standards and Technology. According to a 2018 report by a security-as-a-service vulnerability management service, the web application layer is where the majority of the high and critical risk exposure resides.\textsuperscript{xiv} However, this challenge to promptly patch vulnerabilities may be exacerbated by the fact that patches aren’t immediately available for known vulnerabilities. According to a site that provides comprehensive and timely intelligence on the latest security vulnerabilities, of all those disclosed in 2017, only 76 percent had fixes available.\textsuperscript{xv} This demonstrates how the vulnerability management ecosystem is symbiotic, relying on the
prompt identification of unknown vulnerabilities as well as the technological “fixes” required to mitigate the risk.

## Conclusion

The actor X bears monitoring in the underground due to his association with the sale of these types of exploits. The actor’s strong reputation level reflects his reliability of selling bona fide exploits coupled with customer satisfaction. The high quality of the exploit allows the actor to command a steeper price point and, as such, allows X to be judicious with his sales. This in turn reduces the actor’s footprint in the underground, a move that keeps his profile low.

One-day vulnerabilities like CVE-2018-8453 are extremely valuable to hostile actors that leverage them to fully exploit compromised computers. At this time, many of these vulnerabilities are typically associated with suspected state actors and have been used to support clandestine cyber operations. For example, on October 16, 2018, CVE-2018-8453 was observed being exploited by the “Fruity Armor” advanced persistent threat actor targeting victims in the Middle East region, according to one computer security vendor.xvi

Notwithstanding, vulnerabilities once made public can be used by any actor and against any industry or sector, which makes it incumbent on organizations to quickly apply patches. Assessing risks and prioritizing deployments are key aspects of any organization’s patch management cycle and are a necessary component of a larger cyber security strategy. As one-day and zero-day vulnerabilities continue to become more and more prevalent, proactive development and testing of patch management processes will greatly help reduce an organization’s exposure and remediation efforts.

**Information Cut-Off Date:** December 6, 2018
# Traffic-Light Protocol for Information Dissemination

<table>
<thead>
<tr>
<th>Color</th>
<th>When Should It Be Used?</th>
<th>How May It Be Shared</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>RED</strong></td>
<td>Sources may use TLP: RED when information cannot be effectively acted upon by additional parties, and could lead to impacts on a party’s privacy, reputation, or operations if misused.</td>
<td>Recipients may not share TLP: RED with any parties outside of the specific exchange, meeting, or conversation in which it is originally disclosed.</td>
</tr>
<tr>
<td><strong>AMBER</strong></td>
<td>Sources may use the TLP: AMBER when information requires support to be effectively acted upon but carries the risks to privacy, reputation, or operations if shared outside of the organizations involved.</td>
<td>Recipients may only share TLP: AMBER information with members of their own organization, and only as widely as necessary to act on that information.</td>
</tr>
<tr>
<td><strong>GREEN</strong></td>
<td>Sources may use TLP: GREEN when information is useful for the awareness of all participating organizations as well as with peers within the broader community or sector.</td>
<td>Recipients may share TLP: GREEN information with peers and partner organizations within their sector or community, but not via publicly accessible channels.</td>
</tr>
<tr>
<td><strong>WHITE</strong></td>
<td>Sources may use TLP: WHITE when information carries minimal or no risk of misuse, in accordance with applicable rules and procedures for public release.</td>
<td>TLP: WHITE information may be distributed without restriction, subject to copyright controls.</td>
</tr>
</tbody>
</table>
A Note on Estimative Language

Estimative language is used in order to convey an assessed likelihood or probability of an event, as well as the level of confidence ascribed to a judgment. Assessments are based on collected information (which is often incomplete), as well as logic, argumentation, and precedents. Confidence levels provide assessments of the quality and quantity of the source information that supports judgments.

<table>
<thead>
<tr>
<th>None</th>
<th>Low</th>
<th>Moderate</th>
<th>High</th>
<th>Complete</th>
</tr>
</thead>
<tbody>
<tr>
<td>0-10%</td>
<td>11-49%</td>
<td>50-79%</td>
<td>80-99%</td>
<td>100%</td>
</tr>
</tbody>
</table>

- **Complete**: Totally reliable and corroborated information with no assumptions and clear, undisputed reasoning.

- **High**: Well corroborated information from multiple proven sources, extensive databases, and/or a deep historical understanding of the issue. There are minimal assumptions present. The analytic reasoning is dominated by logical inferences developed through established methodology or multiple analytic techniques. High confidence does not imply an assessment is fact or a certainty.

- **Moderate**: Partially corroborated information from sufficient quality sources (a mix of proven and unproven sources) with some databases and/or historical understanding of the issue. There are assumptions present, of which some should be crucial to the analysis. Reasoning is a mixture of strong and weak inferences developed through simple analytic techniques or an established methodology.

- **Low**: Uncorroborated information from good or marginal sources (mix of semi-proven and unproven sources) with minimal database or historical understanding of the issue. There are many assumptions critical to the analysis. Reasoning is dominated by weak inferences through few analytic techniques.

- **None**: There is no direct information or partially corroborated information to support analytic assessments or judgments, or it is exploratory analysis.
Source and Information Reliability

<table>
<thead>
<tr>
<th>Source</th>
<th>Rating</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>A</td>
<td>Reliable</td>
</tr>
<tr>
<td></td>
<td>B</td>
<td>Usually Reliable</td>
</tr>
<tr>
<td></td>
<td>C</td>
<td>Fairly Reliable</td>
</tr>
<tr>
<td></td>
<td>D</td>
<td>Not Usually Reliable</td>
</tr>
<tr>
<td></td>
<td>E</td>
<td>Unreliable</td>
</tr>
<tr>
<td></td>
<td>F</td>
<td>Can’t Be Judged</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Information</th>
<th>Rating</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>1</td>
<td>Confirmed</td>
</tr>
<tr>
<td></td>
<td>2</td>
<td>Probably True</td>
</tr>
<tr>
<td></td>
<td>3</td>
<td>Possibly True</td>
</tr>
<tr>
<td></td>
<td>4</td>
<td>Doubtfully True</td>
</tr>
<tr>
<td></td>
<td>5</td>
<td>Improbable</td>
</tr>
<tr>
<td></td>
<td>6</td>
<td>Can’t Be Judged</td>
</tr>
</tbody>
</table>

---

i https://docs.microsoft.com/en-us/previous-versions/dotnet/articles/bb625957(v=msdn.10)
iv http://users.ece.cmu.edu/~tdumitra/public_documents/bilge12_zero_day.pdf
v https://lab.getapp.com/zero-day-attacks/
ix https://www.zdnet.com/article/zero-days-fileless-attacks-are-now-the-most-dangerous-threats-to-the-enterprise/
x https://www.darkreading.com/cloud/it-takes-an-average-38-days-to-patch-a-vulnerability/d/d-id/1332638


