HACK IN BO®
Winter 2024 Edition
23ª EDIZIONE

Stealth Domain Generation Algorithm (SDGA): Elevating Malware Stealth and Resilience Beyond Traditional DGA Methods

-=SWaNk=-

Disclaimer

HACK IN BO Winter 2024 Edition
23ª EDIZIONE

MEME

Agenda

- ❑ Whoami
- ❑ Motivation
- ❑ DGA real cases and variations
- ❑ Detection strategies
- ❑ SDGA
- ❑ PoC || GTFO

Agenda

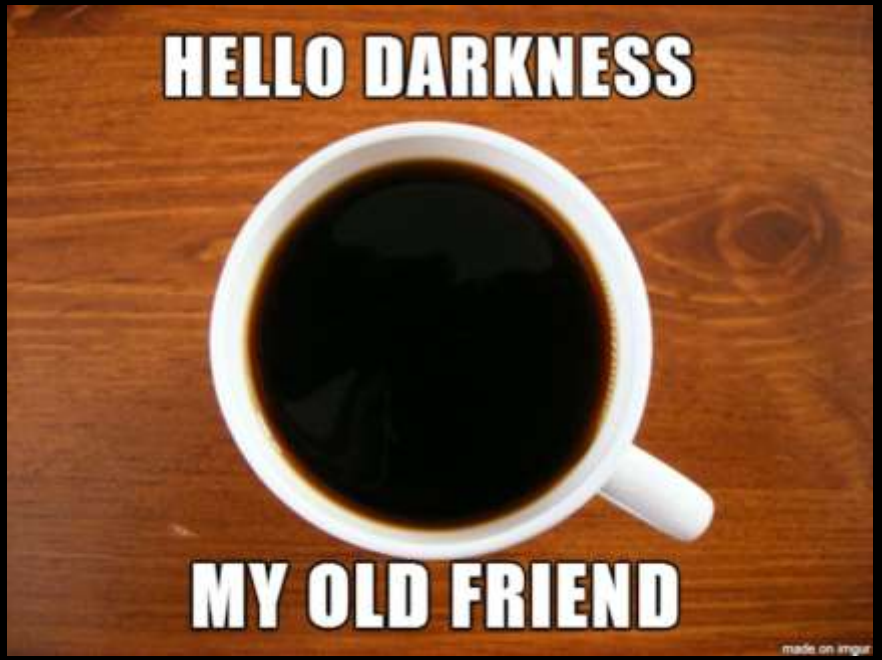
- [ ] Whoami
- [ ] Motivation
- [ ] DGA real cases and variations
- [ ] Detection strategies
- [ ] SDGA
- [ ] PoC || GTFO

I feel at home in Italy because…

- Brazilians don’t cut pasta!

I feel at home in Italy because…

- Brazilians can't live without good and strong coffee…



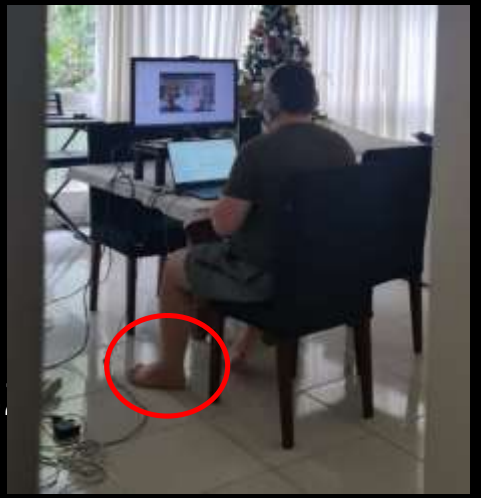
I feel at home in Italy because…

- La madre di mia nonna era italiana, quindi ho un po' di sangue italiano nelle vene. Maria Raphaella Torelli Bazzarelli (Campania)

I feel at home in Italy because…

- We fought together in the “Battaglia del Monte Castello” – World War II
- “a cobra vai fumar” Smoking Snakes (Army)
- “Senta a Púa!” 1st Fighter Group (Air Force)
- Sabaton song: “Smoking Snakes”

whoami



- Rafael Salema Marques (SWaNk)
- Malware coder / Researcher / Privateer
  - Mabouia Ransomware OSX PoC
  - 29a issue #7
  - Phrack Magazine Issue #71
  - LOLBAS => Desk.cpl (MITRE ATT&CK®: T1218.011: Rundll3
  - Academic research: Pivot & rootkit detection
- Red Team Leader
- Malware Analysis & Reverse Engineering
- Malware Development (Red Team Engagement)

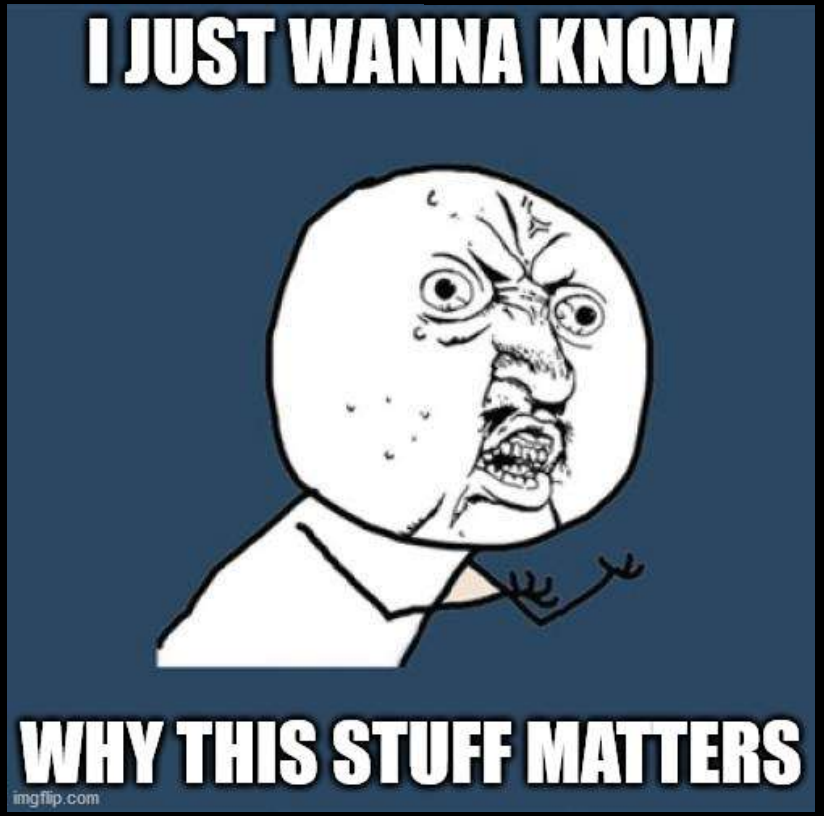
Agenda

- ❑ Whoami
- ❑ Motivation
- ❑ DGA real cases and variations
- ❑ Detection strategies
- ❑ SDGA
- ❑ PoC || GTFO

Motivation

Why is this relevant for a Red Team engagement?

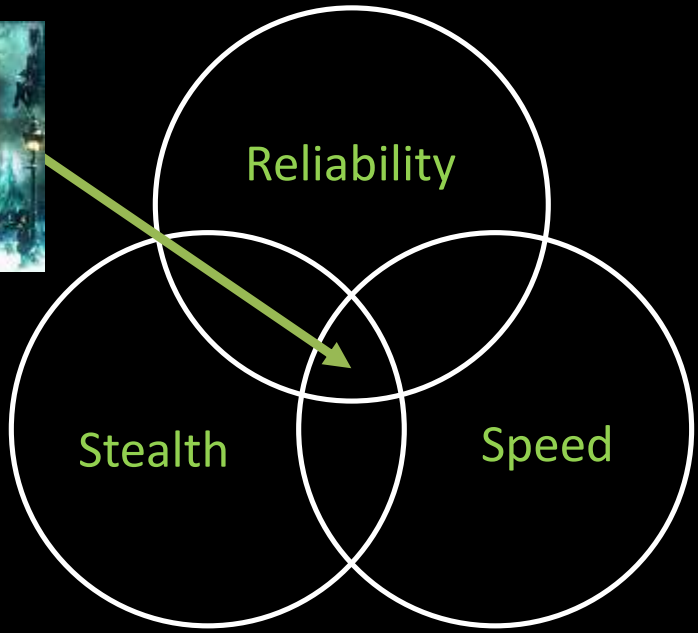
- A C2 channel is necessary to support several malware functionalities
- Eventually your C2 ~~can~~ will be detected and taken down and DGA can be useful recovering control of your implant
- But… Most DGA strategies generate a lot of noise



Motivation

In a modern real world scenario, a malware C2 architecture must trade… Normally you can pick 2…

- **SDGA can help with…**
  - **Reliability: Fallback mechanism**
  - **Stealth: avoid DGA noise**



Agenda

- ❑ Whoami
- ❑ Motivation
- ❑ DGA real cases and variations
- ❑ Detection strategies
- ❑ SDGA
- ❑ PoC || GTFO

Classic DGA

- MITRE Definition:
  - "Adversaries may make use of Domain Generation Algorithms (DGAs) to dynamically identify a destination domain for command and control traffic rather than relying on a list of static IP addresses or domains. This has the advantage of making it much harder for defenders to block, track, or take over the command and control channel, as there potentially could be thousands of domains that malware can check for instructions."

Classic DGA

- Typical DGA 3 componentes:
  - Generation “seed”
    - Time based
    - Collection of unpredictable information (lottery, stock…)
  - Domain name generation algorithm based on the seed
  - Various top-level domains (.com, .net, .org…)
  - Avoids hardcoded domains inside the malware

DGA real cases

- Naikon APT (Time based)
  - Chinese APT group
  - Aria-body backdoor
  - Domain len: 8 to 21 chars
  - Change daily (flaw)
- Example using seed 12345:
  - 27 OUT 2024:
  - bxsgllccn.org
  - Today:
  - jdeozhgujhggztwaxlc.com

```
def DGA_method(seed_value):
    domain = ""
    tld = [".com", ".org", ".info"]
    ta = time.localtime(time.time())
    temp1 = math_s(ta.tm_year)
    temp2 = math_s(dword(temp1 + ta.tm_mon + 0x11FDA))
    temp3 = math_s(dword(temp2 + ta.tm_mday))
    temp4 = math_s(dword(seed_value + temp3))
    temp5 = math_s(dword(temp4 + 9))
    length = (temp5 % 0xe) + 8
    if length > 0:
        for i in range(length):
            temp6 = math_s(i + temp5)
            domain += chr ( ( temp6 % 0x1a) + 0x61)
            temp5 = math_s(dword(temp6 + 0xcdcdef))

    domain += tld[temp6 % 3]
    print(domain)
```

DGA real cases

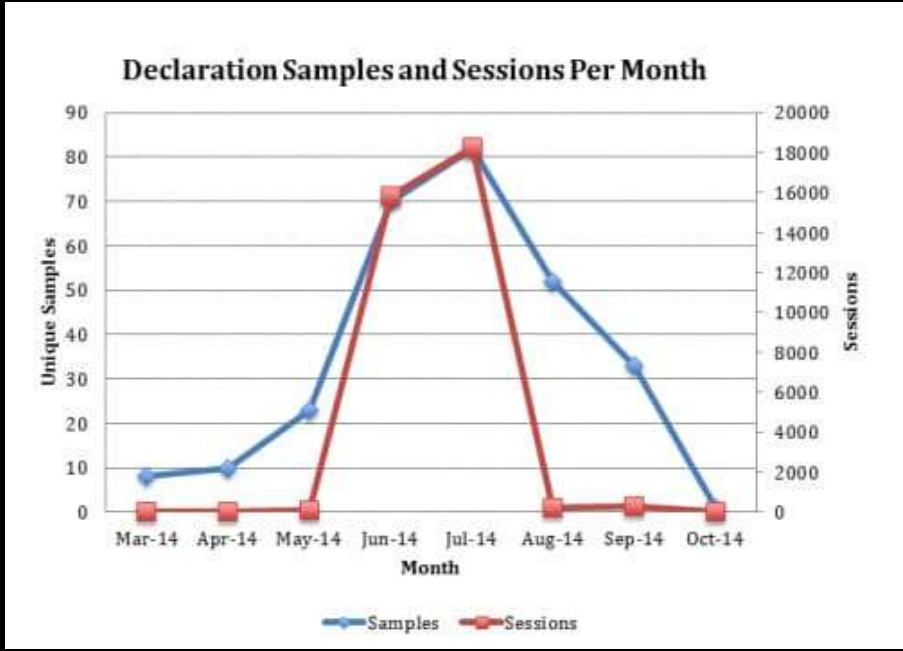
- Rovnix (Time and collection based)
  - Sophisticated banking trojan with bootkit capabilities
- Seeds
  - US Declaration of Independence as seed
  - https://www.constitution.org/usdeclar.txt
  - GNU Lesser General Public License
  - https://www.gnu.org/licenses/lgpl-3.0.txt
  - RFC 4288
  - https://www.ietf.org/rfc/rfc4288.txt

DGA real cases

- Rovnix (Time and Collection based)
- Generated domains
  - tosecureonweestablishment.com
  - toformidablerepeated.com
  - alllawstheheagesusurpations.com
  - createdtheywhencolonies.com
  - absolutesopassofhave.com
  - civiltheirtheinconsanguinity.com
  - ofpublichistoryourabdicated.com

DGA real cases

- Rovnix (Time and Collection based)
- Fun fact
  - hits to The constitution Society became suspicious
  - The blue team could monitor the campaign spread
  - “declaration generation algorithm” ☺
- DGA strategy drawback
  - The malware operator do not control the seed data

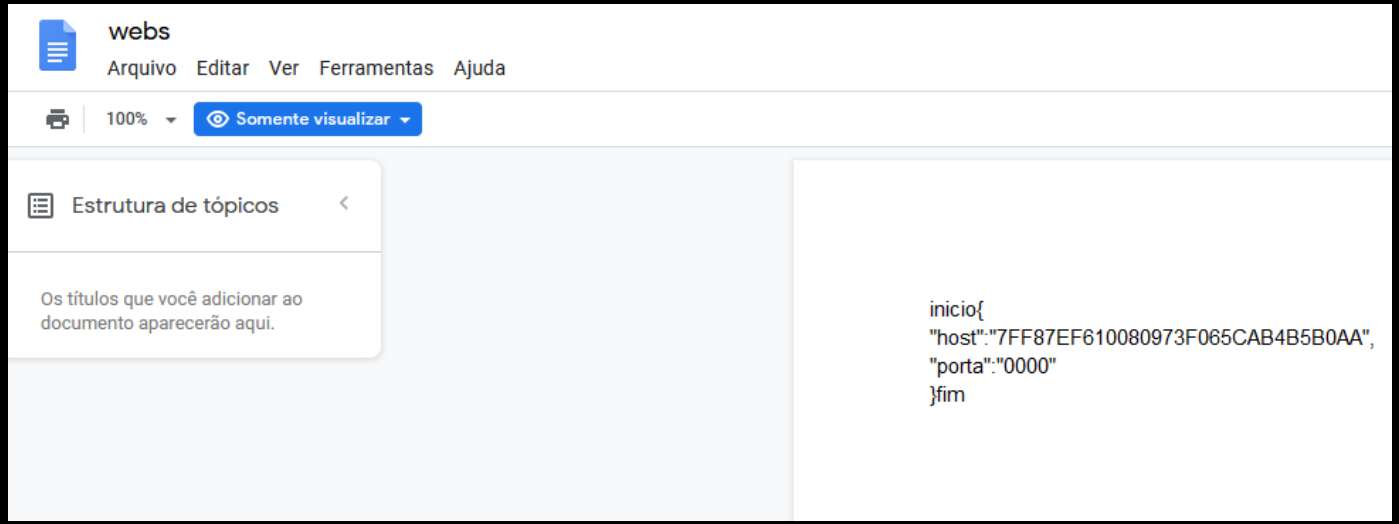


DGA real cases

- Javali / Guildma (Time based)
  - MaaS Brazilian banking trojan
  - Targeting local banks for years
  - Global expansion (LATAM and Europe)
  - Payloads hosted within Youtube and FB posts
  - Configurations hidden into GoogleDocs
- generate thousands of daily URLs (no connection)
  - g2ha14u2m2xe12.com.de
  - ghcco980m1zy9.org
  - 04autogestor.ml

DGA real cases

- Javali / Guildma (Time based)
  - Uses DGA if the Google Docs hardcoded host is down (recovery)



DGA real cases

- Guildma / Astaroth (Time based)
  - Download malware configuration on Youtube and Facebook pages

Agenda

- ❑ Whoami
- ❑ Motivation
- ❑ DGA real cases and variations
- ❑ Detection strategies
- ❑ SDGA
- ❑ PoC || GTFO

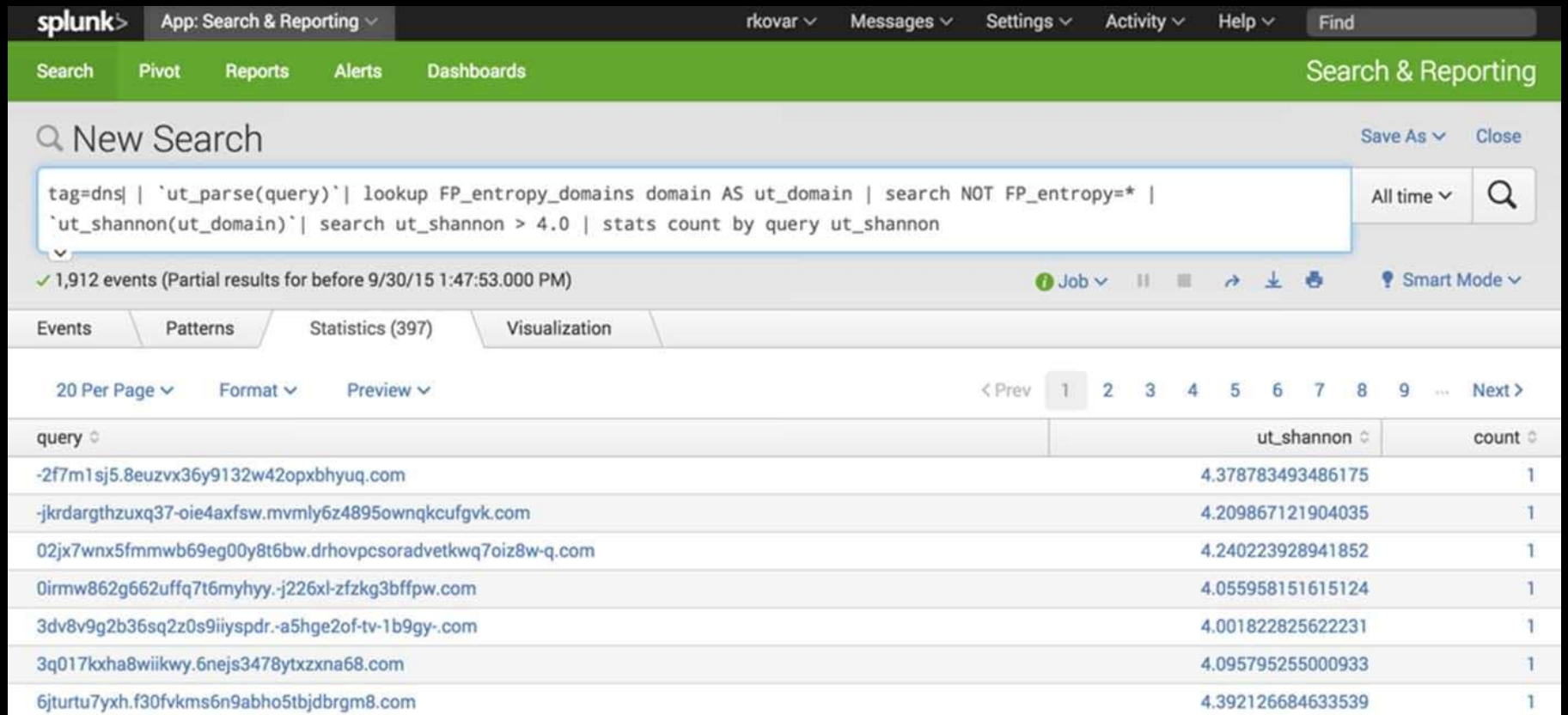
Detection strategies

- Random domain names generation

- Can lead to IoC:
  - Several time based DGA tend to generate high entropy domains
  - Shannon entropy: "… a measure of uncertainty in a random variable"
  - Detection metric: the higher the entropy, the more likely it is to be malicious.

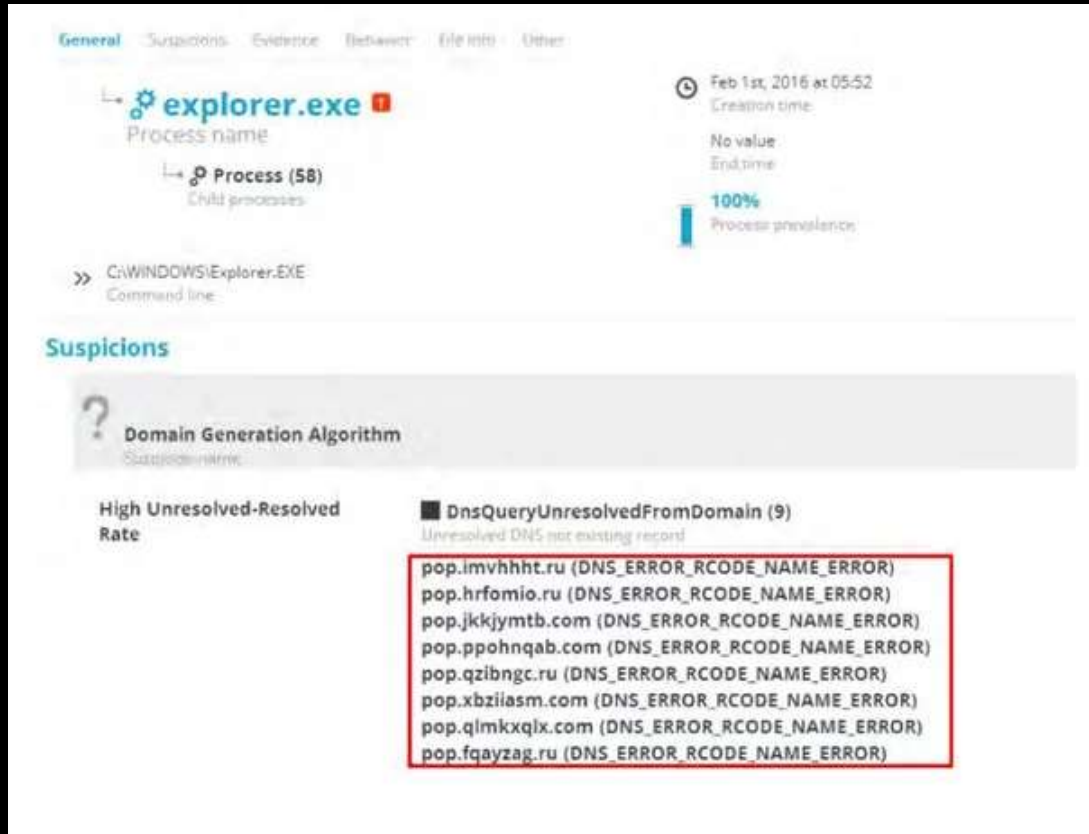
$$H = -\sum p(x) \log p(x)$$

Detection strategies



Detection strategies

- high unresolved domain rate
- Can lead to IoC:
  - When malware attempts to connect to some unregistered domains, it will cause network anomaly



Agenda

- ❑ Whoami
- ❑ Motivation
- ❑ DGA real cases and variations
- ❑ Detection strategies
- ❑ SDGA
- ❑ PoC || GTFO

SDGA

- Stealth Domain Generation Algorithm
- Leverages famous third-party services to host C2 domain information
- Requires a service that can provide:
  - User controlled data
  - Data accessible to the malware without login
- Advantages
  - reduces network noise
  - improves stealth by blending with legitimate traffic from widely trusted platforms “Hiding in plain sight”

SDGA real cases

- Grandoreiro (Time based)
  - The code suggests that the campaign is being managed by various operators.

```
System::__linkproc__ LStrCmp(*(*this)->operatorId, "01");
if ( strMatch )
{
  getDate(&currDate);
  Sysutils::Trim(currDate);
  unknown_libname_1044(*off_B85504[0]);
  get_str(0x117, &encSeed);
  decryptStr(0, encSeed, &decSeed);
  System::__linkproc__ LStrLAsg(&seedUrl, decSeed);
  calcUrl(currDate, seedUrl, &gsitesPath);
  System::__linkproc__ LStrCat3(&finalGsitesPath, "zemad", gsitesPath);
  Sysutils::AnsiLowerCase(finalGsitesPath);
}
```

SDGA real cases

- Grandoreiro (Time based)
  - The generated path will then be contacted to collect information about the C2 server.

ID	Operator	Key	Date	Generated path
01	zemad	jkABCDEefghiHla4567JKLMN3UVWpqrst2Z89PQRSTbuvwxyzXYFG01cdOlmno	16Mar0	zemadhjui3nfz
02	rici	jkABCDEefghFG01cdOlmnopqrst2Z89PQRiHla4567JKLMN3UVWXYSTbuvwxyz	16Mar0	ricigms0rqfu
03	breza	01cdOlmnopqrst2Z89PQRSTbuvwxjkABCDEefghiHla4567JKLMN3UVWXYFGyz	16Mar0	brezasqvtubok
04	grl2	mDEefghiHla4567JKLMNnopqrst2Z89PQRSTbuv01cdOlwxjkABC3UVWXYFGyz	16Mar0	grl25ns6rqhk
05	rox2	567JKLMNnopqrst2Z89PQmDEefghiHla4RSTbuv01cdOlwxjkABC3UVWXYFGyz	16Mar0	rox2rpfseenk
06	mrb	567JKLMNnopqrst2Z89PQmDEefghiHla4RSTbuv01cdOlwxjkABC3UVWXYFGyz	16Mar0	mrbrpfseenk

SDGA real cases

- Grandoreiro (Time based)
  - The google Doc will have the IP and port information.

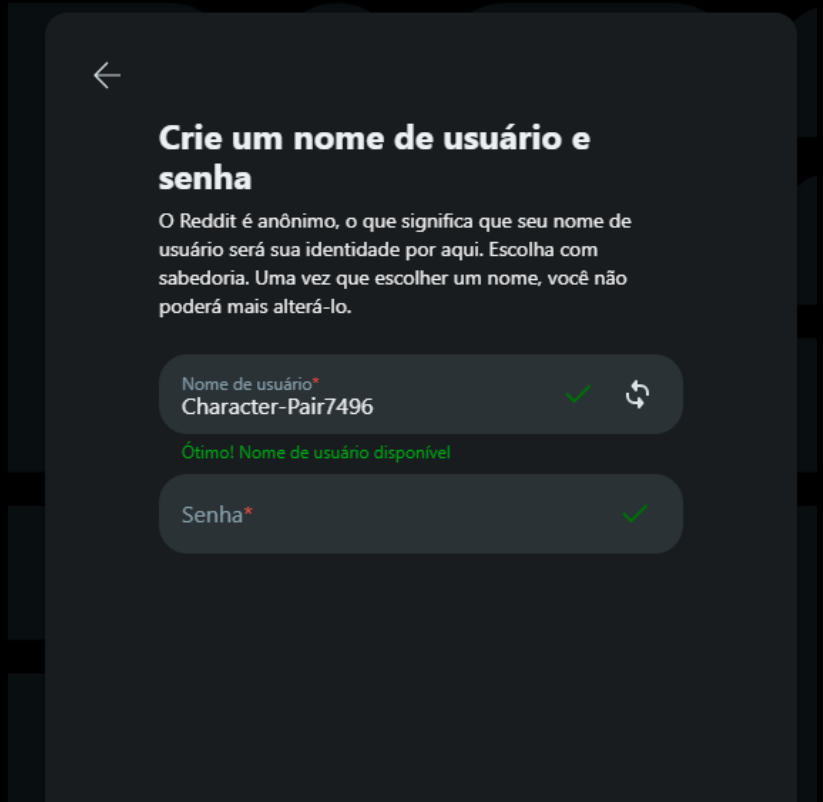
SDGA real cases

- IMHO, data must fit the context to increase the campaign's detection time
  - A shellcode is not compatible with a youtube post…
  - A single IP;PORT; is more likely to appear suspicious compared to a text paragraph

SDGA

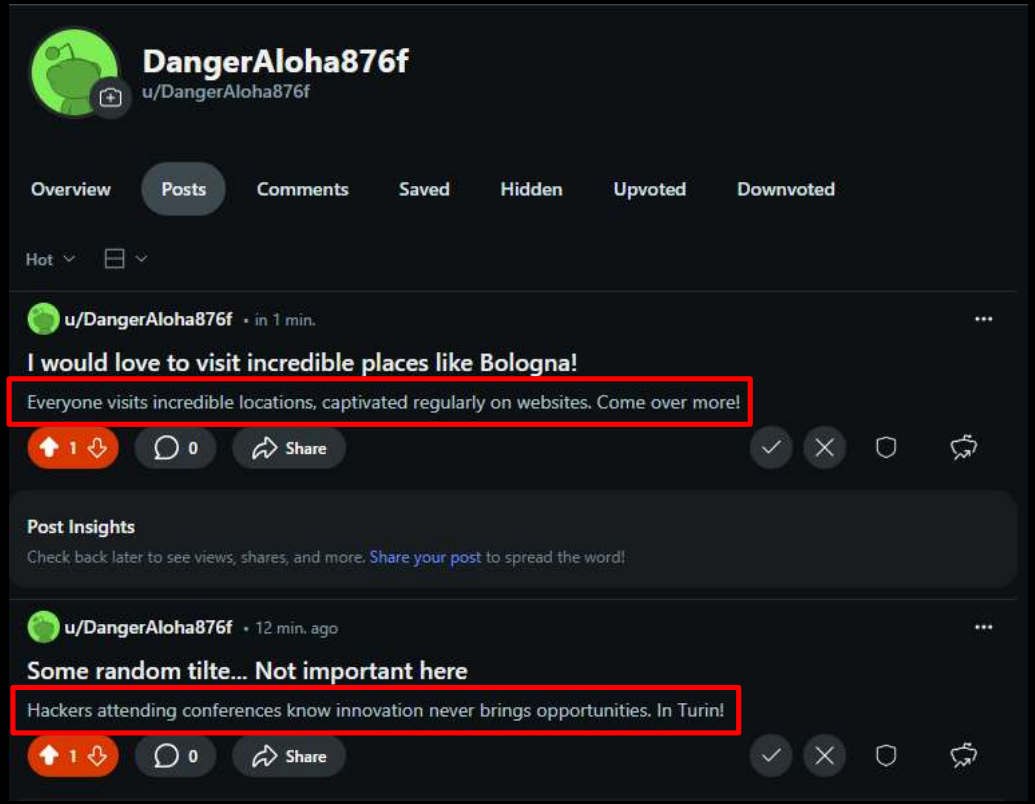
- Our Stealth Domain Generation Algorithm implementation
- Web service => Reddit.com
- Username generation algorithm
  - Time based / md5 hash / dictionary english words
- Domain extraction algorithm
  - First word letter
  - Consider "."
  - Data compatible with the environment (Important!)

- Why Reddit?
  - Easy to create user
  - You can choose the username
  - Many other would fit…
  - Nothing against reddit 💔

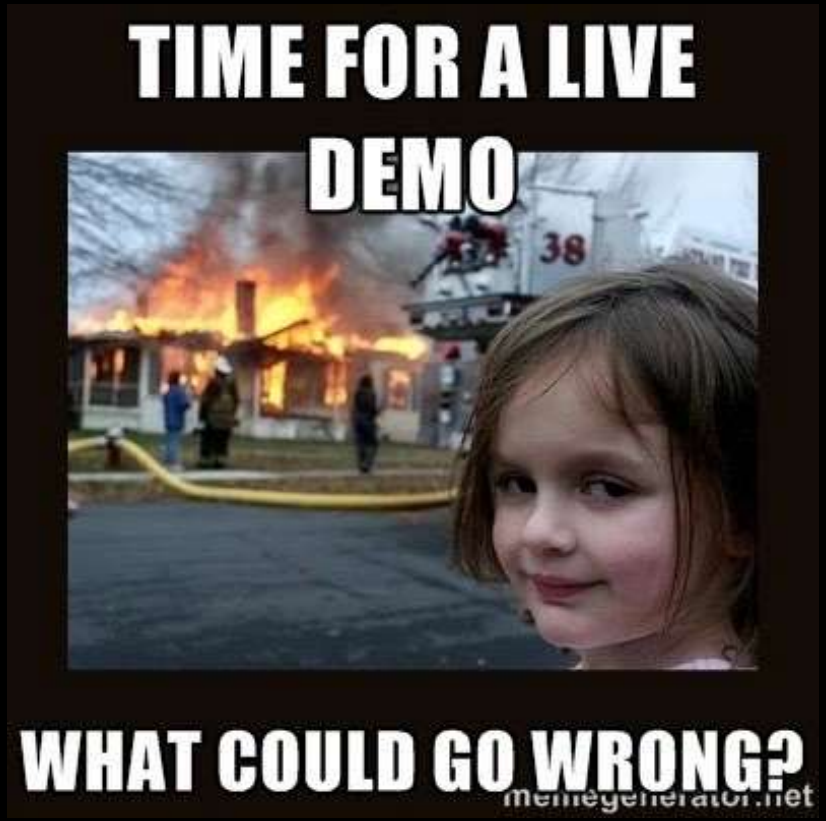


SDGA

- Extraction
  - Parse all posts
  - Brute force every <p> tag
  - If the extraction of the <p> tag content results in a valid domain, it is collected and will be used to call back home.



Proof of Concept



:(

Your PC ran into a proble
just collecting some erro
you.

20% complete

For more information about this i

If you call a support person, give them th

Stop code: CRITICAL_PROCESS_DIED

References

HACK IN BO Winter 2024 Edition
23ª EDIZIONE

DGA

- https://unit42.paloaltonetworks.com/threat-brief-understanding-domain-generation-algorithms-dga/
- https://unit42.paloaltonetworks.com/rovnix-declaration-generation-algorithm/
- https://securelist.com/the-tetrade-brazilian-banking-malware/97779/

Shannon entropy

- https://www.splunk.com/en_us/blog/security/random-words-on-entropy-and-dns.html

That's all folks!

Telegram: @swankvx
Twitter: @pegaBizu
Email: contato@vectorcrow.com

Questions?!

HACK IN BO®
Winter 2024 Edition
23ª EDIZIONE