In the Lair of the Beholder

Kyle Maxwell
@kylemaxwell
kmaxwell@verisign.com

SANS DFIR Summit
Austin, Texas
July 2015

How this got started

“Beholder” is Product Identity of Wizards of the Coast

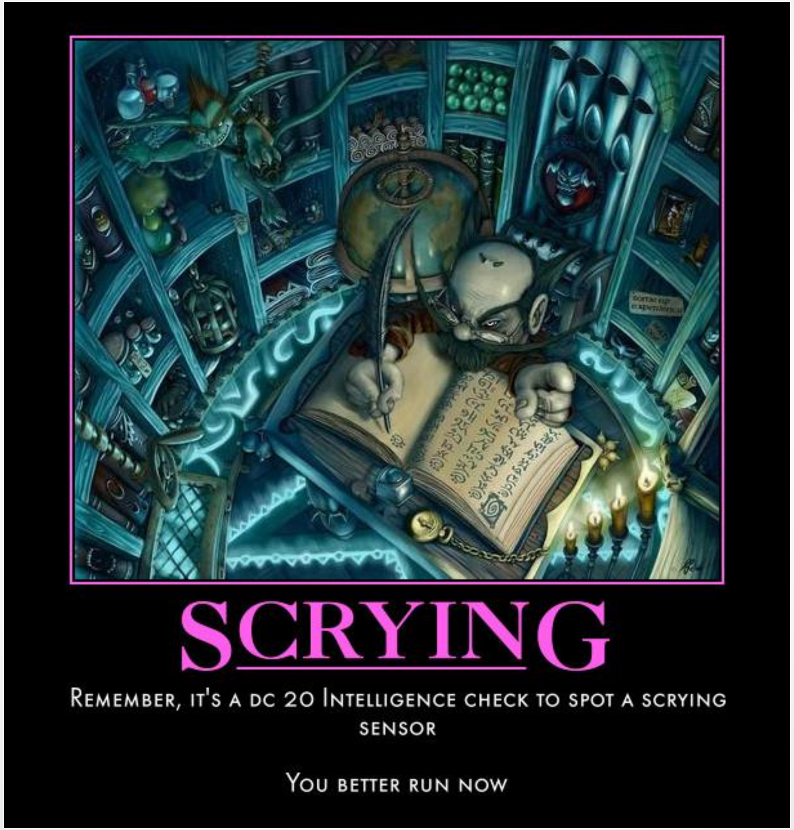
https://speakerdeck.com/krmaxwell/in-the-lair-of-the-beholder

External IOCs

How to look?

- Blacklists
- WHOIS
- Search engine automation
- Malware repositories

OSINT is a lot like this


SCRYING
Remember, it's a dc 20 Intelligence check to spot a scrying sensor
You better run now

Blacklists

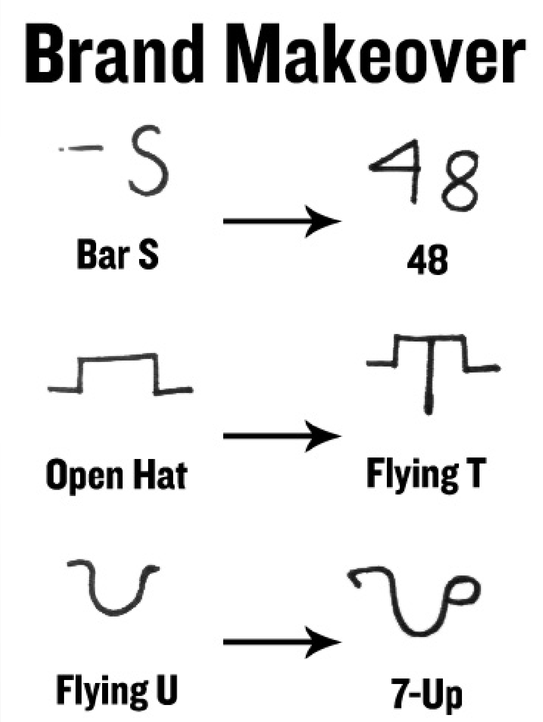
Check popular “threat intel data feeds” using Combine plus Flail

https://github.com/mlsecproject/combine
https://github.com/krmaxwell/flail

Games Workshop

WHOIS

Registration of domains relevant to brand or organization name



http://modernfarmer.com/2013/06/cowglyphics-decoding-cattle-brands/

Search Engine Automation

Custom Search Engine for paste sites

Google Alerts for key email addresses (executives, honeytokens, etc.)

Malware Repositories

YARA: “The pattern matching swiss knife”
http://plusvic.github.io/yara/

“Antivirus that you update using `git pull`”

~ @tomchop_

YARA Example (super naïve)

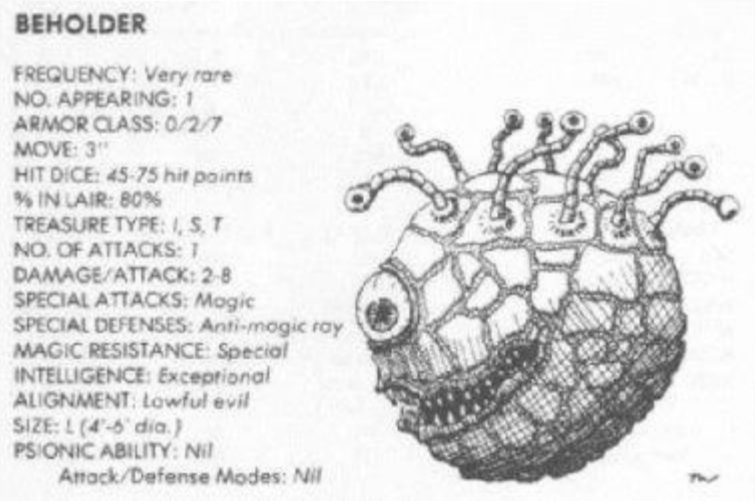
```
rule verisign_email
{
    strings:
        $email_domain = "@verisign.com"
        $common_email = "CPS-requests"

    condition:
        $email_domain and not $common_email
}
```

Automation

“Scumblr is a web application that allows performing periodic searches and storing / taking actions on the identified results.”

https://github.com/Netflix/Scumblr

Lesson: Start off simple



BEHOLDER

FREQUENCY: *Very rare*
NO. APPEARING: *1*
ARMOR CLASS: *0/2/7*
MOVE: 3"
HIT DICE: *45-75 hit points*
% IN LAIR: *80%*
TREASURE TYPE: *I, S, T*
NO. OF ATTACKS: *1*
DAMAGE/ATTACK: 2-8
SPECIAL ATTACKS: *Magic*
SPECIAL DEFENSES: *Anti-magic ray*
MAGIC RESISTANCE: *Special*
INTELLIGENCE: *Exceptional*
ALIGNMENT: *Lawful evil*
SIZE: *L (4'-6' dia.)*
PSIONIC ABILITY: *Nil*
Attack/Defense Modes: *Nil*

Lesson: Evolve or die

Lesson: Work with others

Professionals can usually provide richer details.

Discussion

Thanks!

@kylemaxwell
kmaxwell@verisign.com