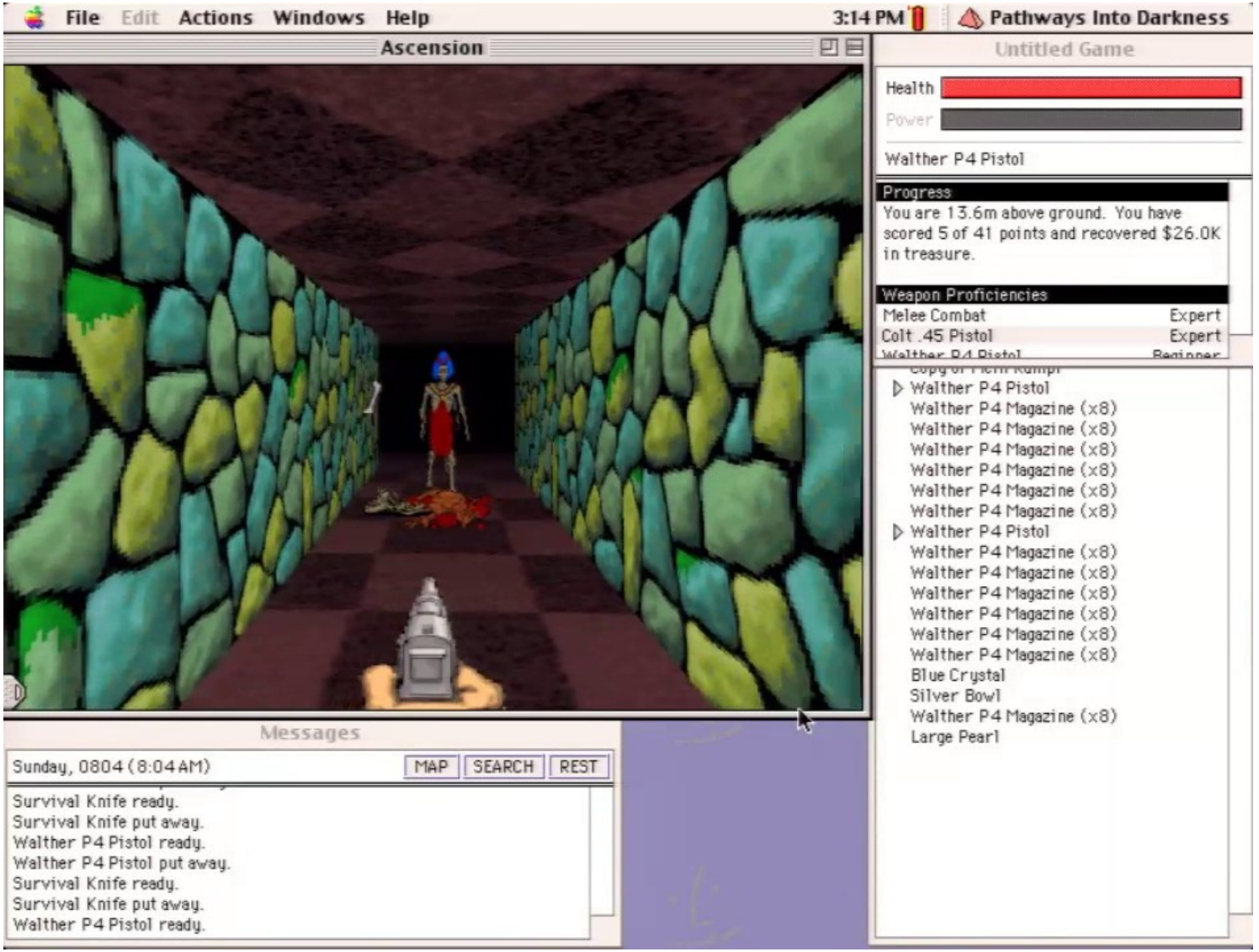
Pathways Into Darkness

Hunting for Adversary Behaviors Atop The Pyramid Of Pain

whois

- Kyle Gervais
- Previous: SOC Analyst at a Fortune X
- Threat Intelligence Analyst at a Fortune X
- Automation Elf
- Friend of Felines
- Definitely didn’t choose his topic to make a reference to an old adventure horror game

But since it came up...



IOAs, IOCs, Anemones?

- Indicator of Compromise
  - Typically discrete values
  - Tied to a known actor or campaign
  - Relatively high confidence
  - “Oh, That’s Bad”
  - Example:
    - FTP connections to a domain known to be used by APT FuzzySnugglyDuckling for exfiltration: “toteslegit[.]rly”

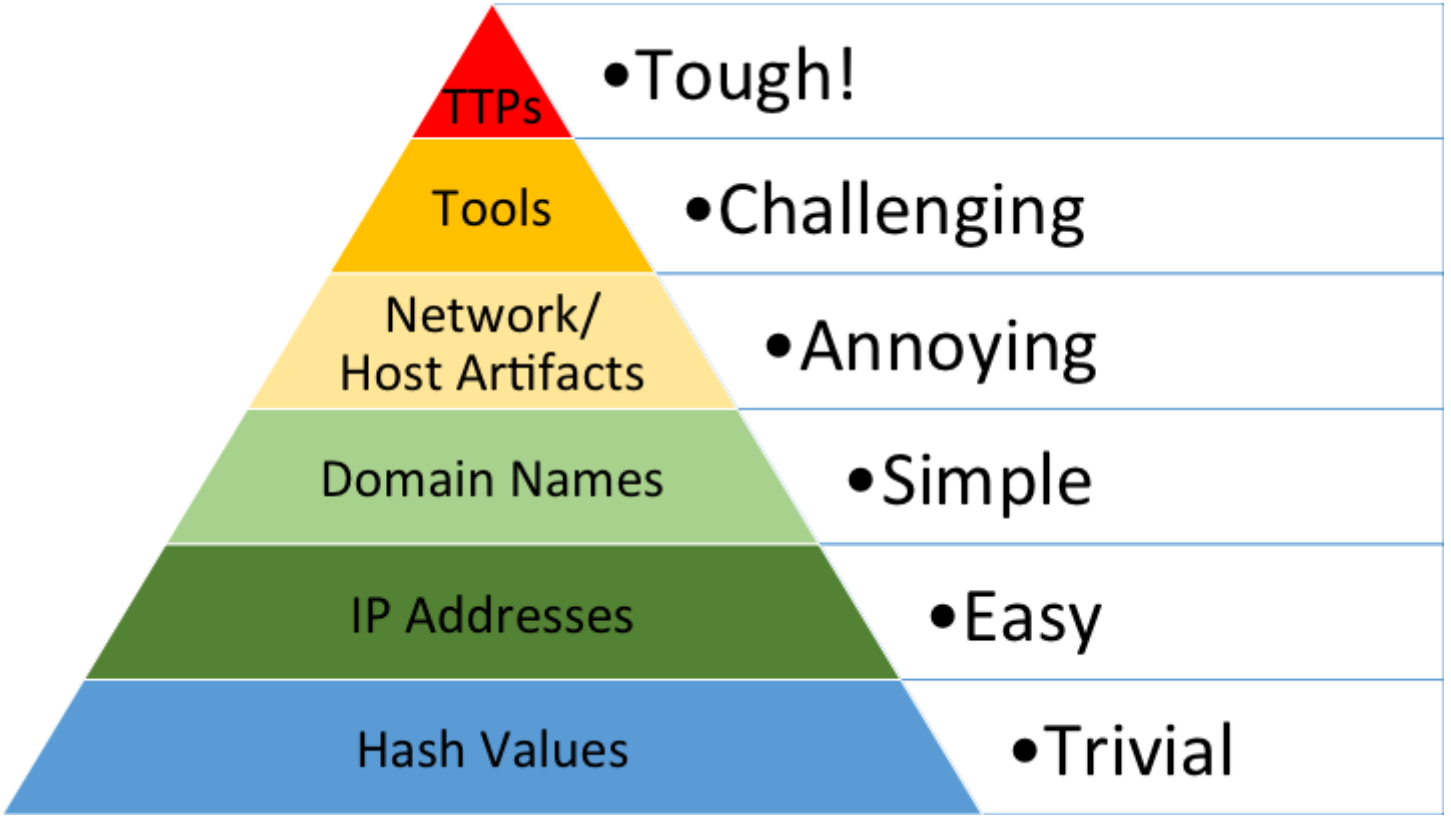
IOAs, IOCs, Anemones?

- Indicator of Attack
  - Not concrete, but can lead to earlier detection
  - A launching point for hunting
  - Potentially low fidelity
  - “Huh, That’s Weird”
  - Example:
    - You see a host on your DMZ trying to talk a server used by your product development team to store alpha builds

IOAs, IOCs, Anemones?

Joel Carnat / Dutch Grown

“Pyramid of Pain”



http://detect-respond.blogspot.com/2013/03/the-pyramid-of-pain.html

Hash Values

- A (semi) unique identifier for a specific file
- “pandas eat bamboo!”
- MD5
  - 27060632c83f609446fe4fc3e1906c9a
- SHA-1
  - 9efcb7fdbd1760abfd410b642df8e9d3106f710a
- SHA-256
  - ad023f382312edc53f693bb337adb890bd42d48997b8eecb64fdce3208daff12

IP Addresses

- IPv4
  - 203.72.42.137
- IPv6
  - FE80:CD00:0000:0CDE:1257:0000:211E:729C
- Put simply, the street address of a computer

Domain Names

- google.com
- mail.google.com
- fuzzysnugglyduckling.org
- gmail.com.toteslegit.rly
- panda1.dynamicdnsservice.com
- panda2.dynamicdnsservice.com

Network & Host Artifacts

- Filenames of malicious word documents
- A user agent string used when making a network connection
- A registry key set by malware to enable persistence
- Where a temp file gets stored during installation

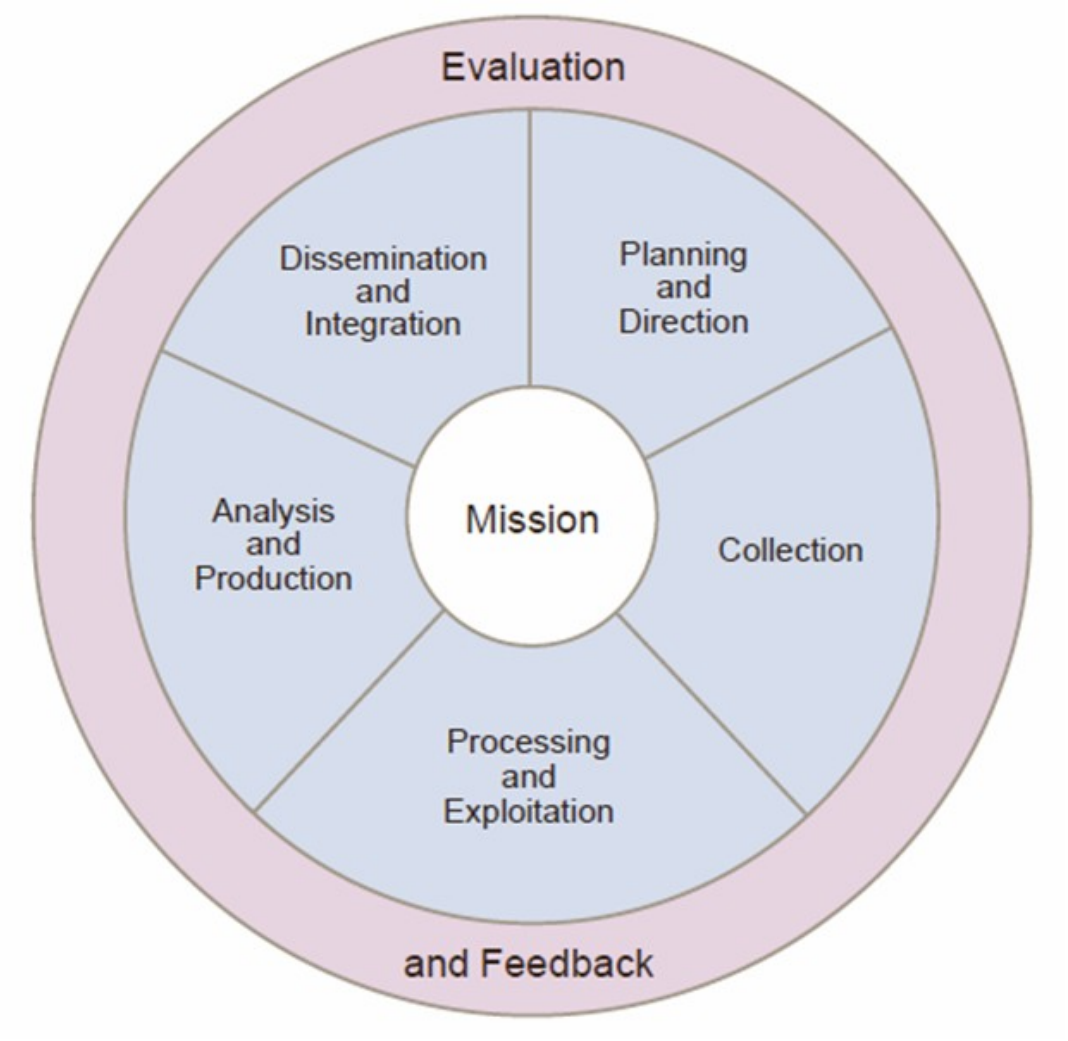
Tools

- Example - Non-customized versions of:
  - Mimikatz
    - Credential theft tool to enable pass-the-hash
  - CobaltStrike/Metasploit
    - General attack platform with different modules

Tactics, Techniques, Procedures

- Example:
  - Spearphishing a target employee, using a malicious PDF that contains a link to an executable disguised as a zip file.
- Example mitigations:
  - Heuristic detection of spearphishing
  - Detecting files whose headers don’t match their file extension
  - Detecting network connections initiated by a PDF reader

The Intelligence Cycle

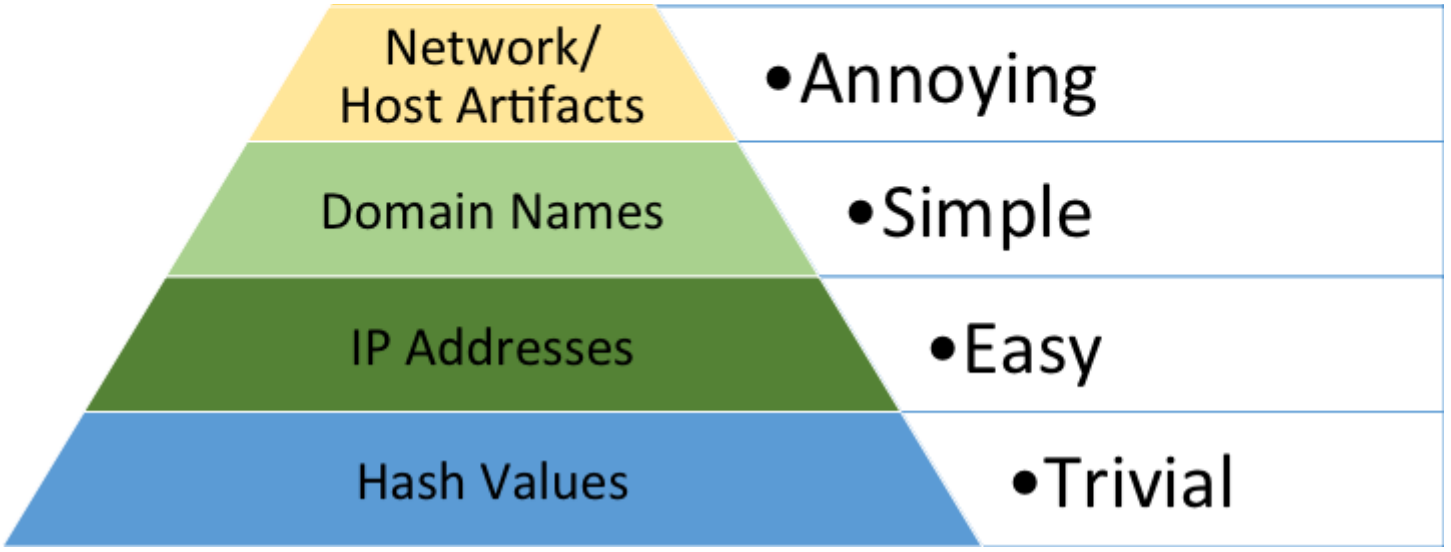


Join Intelligence / Joint Publication 2-0 (Joint Chiefs of Staff)

Challenges SOCs Face

- Alert fatigue
- High volume of intelligence reporting
- Limited Resources
- “Hunt for Badness”

Base of The Pyramid

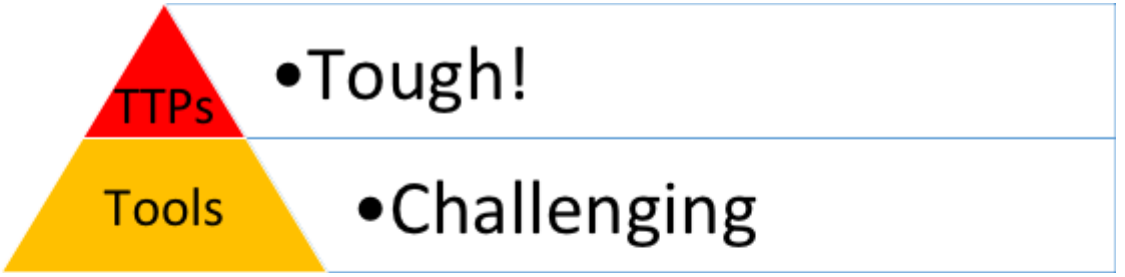


http://detect-respond.blogspot.com/2013/03/the-pyramid-of-pain.html

Current Strategies

- Manual (Example)
  - Tier 1 ingests IOC section
  - Tier 2 searches for activity
  - Someone builds alert
- Automated
  - Parse out atomic indicators
  - Search for activity
  - If activity is found:
  - SOC/CTI/DFIR run to ground, build alert

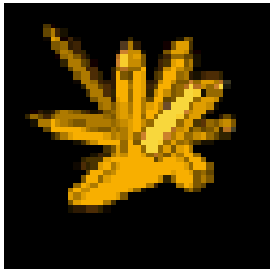
Top of The Pyramid



http://detect-respond.blogspot.com/2013/03/the-pyramid-of-pain.html

Necroliteracy

PATHWAYS INTO DARKNESS



Yellow Crystal

The yellow crystal seems to hum in your hand.

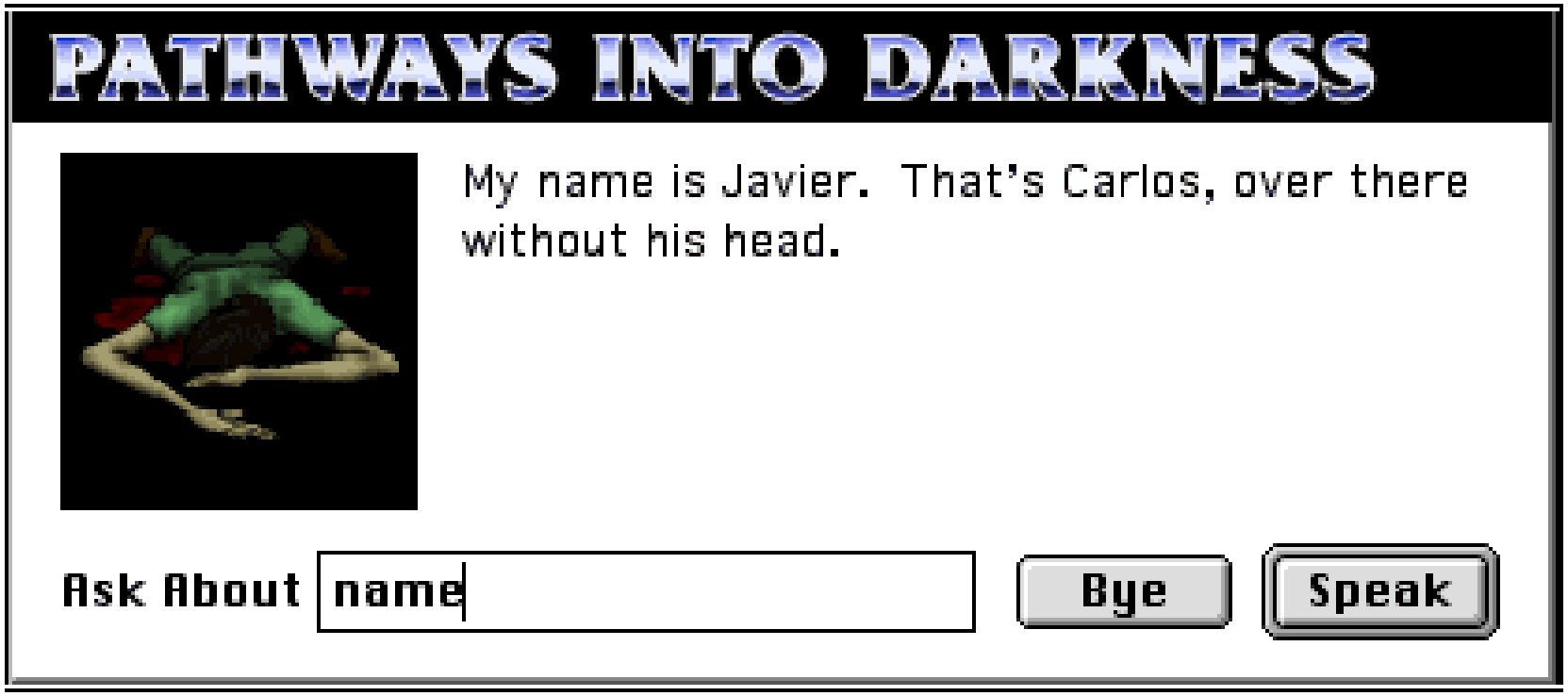
To begin charging the yellow crystal, double-click on it. Discharge it by pressing TAB while standing over a dead person to talk to them.

OK

Reading Strategies

- Try to recognize patterns:
  - Behaviors
  - Naming conventions
  - Subject line flavors
- Understand the attack
- Consider the context
- Think specifically
- Think broadly

Example 1: Javier



ICEBRG Report

- “Adobe Flash Zero-Day Leveraged For Targeted Attack In Middle East”
- https://www.icebrg.io/blog/adobe-flash-zero-day-targeted-attack
- Google: icebrg flash

ICEBRG Report

Indicator	Description
0b4f0d8d57fd1cb9b4408013aa7fe5986339ce66ad09c941e76626b5d872e0b5	SHA256 hash of the document lure.
185.145.128[.]57	IP Address of shared hosting provider (abelons[.]com) hosting payloads for exploit chain.
people.dohabayt[.]com	Domain used for various stages of the exploit chain.
6535abc68a777b82b8dca49ffbf2d80af7491e76020028a3e18186e1cad02abe	SHA256 of SSL certificate observed on malicious infrastructure. https://crt.sh/?id=482419008
internationsplanet[.]com	Domain associated with SSL certificate observed on malicious infrastructure.

Figure 11: Table of atomic indicators

ICEBRG Report

- Base of the Pyramid
  - File hash of sample
  - File hash of certificate
  - IP Address
  - Two Domains
- Top of the Pyramid
  - ?

ICEBRG Report

The SWF stages log data to the URL identified as 'stabUrl', which is on the same command-and-control server. The URI is constructed by appending a random value onto a format string (Figure 6), whose values will indicate the current function, and progress within the function, that is transmitted to track successes and failures. For example, the value reported after successful retrieval of the first stage is '0-0-0'.

```
stabUrl + “%d-%d-%d.png?x=”+ Math.random()
```

Figure 6: Computation of the stabURL

Stop! Regex Time

- Regular Expression
- Means of expressing a text pattern
- Some basics:
  - \d is numbers
  - \w is “word characters”
  - [a-zA-Z] is a character class with ranges
  - . is “anything”
  - * is the previous character repeated zero or more times
  - + is the previous character one or more times
  - ? signifies the previous character is optional

ICEBRG Report

```
stabUrl + “%d-%d-%d.png?x=”+ Math.random()
```

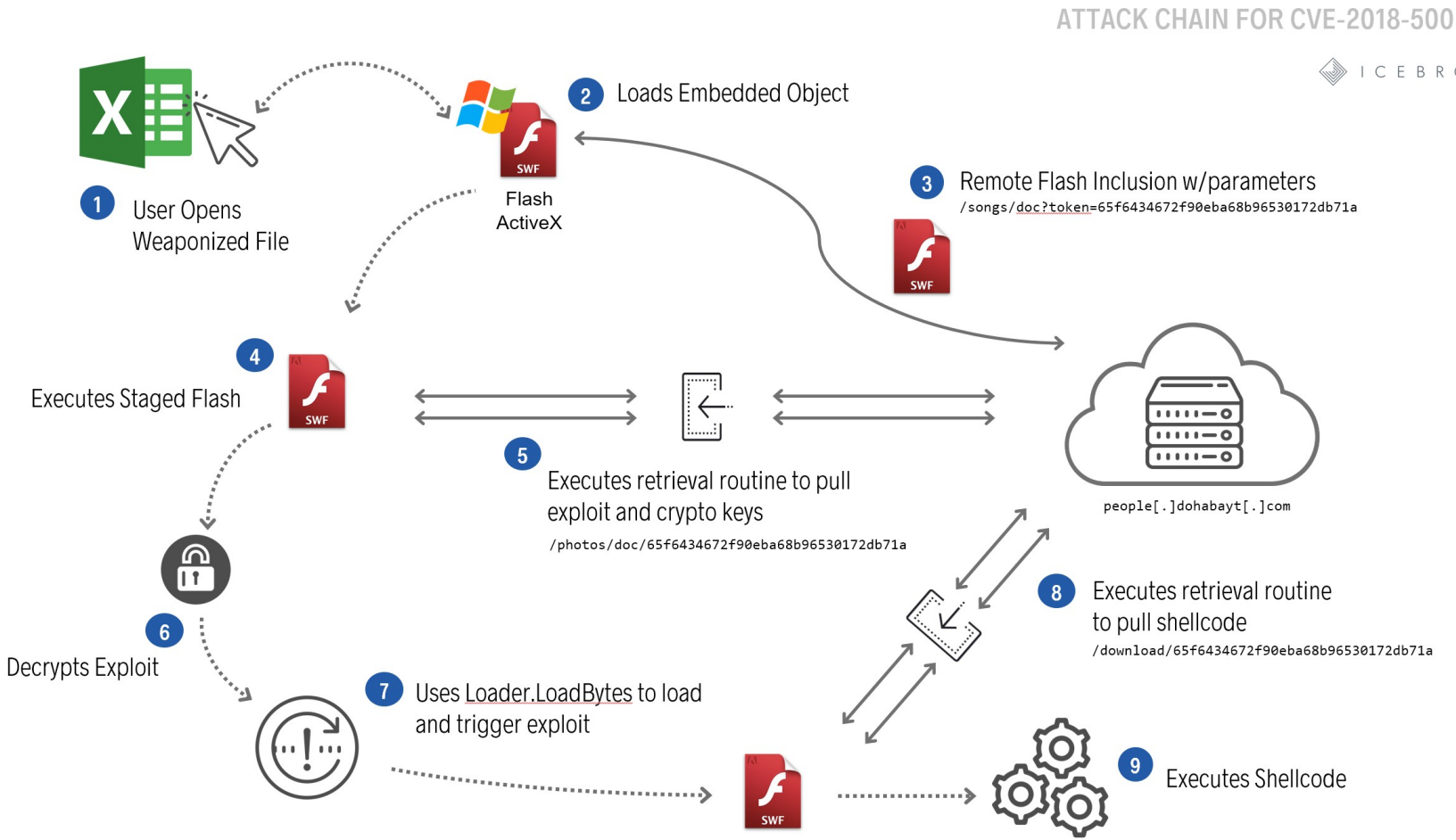
Figure 6: Computation of the stabURL

URL= \d-\d-\d-\.png\?x=[\d\.]+$

ICEBRG Report

- Base of the Pyramid
  - File hash of sample
  - File hash of certificate
  - IP Address
  - Two Domains
- Top of the Pyramid
  - URL= \d-\d-\d-\.png\?x=[\d\.]+$

ICEBRG Report



ICEBRG Report

- Base of the Pyramid
  - File hash of sample
  - File hash of certificate
  - IP Address
  - Two Domains
  - Inclusion parameters
- Top of the Pyramid
  - URL= \d-\d-\d-\.png\?x=[\d\.]+$
  - Office product initiating a connection using ActiveX
  - ActiveX spawning Flash

ICEBRG Report

- Naming scheme: related city + regional job site
- How would this look if your org is the target?
- sacramentodice.com?
- phoenixninjajobs.org?
- phoenixlinkedin.com?

ICEBRG Report

- Top of the Pyramid
  - URL= \d-\d-\d-\.png\?x=[\d\.]+$
  - Office product initiating a connection using ActiveX
  - ActiveX spawning Flash
  - Domain naming convention used by the actor

ICEBRG Report

- **Use of Newly Registered and Low Reputation Infrastructure**: The domains utilized in this attack chain are very recently registered domains (Figure 12) and leverage low reputation hosting providers and registars that commonly host malicious sites. The hosting provider Abelons has been repeatedly included on spamhaus and abused by attackers to deliver malicious content.
- **Staged Download of Flash**: During the attack chain, the weaponized document loads the malicious Flash object through remote loading resulting in observable HTTP traffic resulting with the header "x-flash-version" pulling a secondary Flash object (Figure 8).
- **Use of Newly Created "Let's Encrypt" Certificate**: A certificate observed being hosted on malicious infrastructure, likely used for some aspect of a malicious campaign, is a newly observed certificate (Figure 12) from a free provider that contains a hostname mismatch with the server itself.
- **Office Document with Embedded Flash Using Remote Inclusion:** The document utilized in the attack utilizes an uncommon method of embedding Flash and such methods, particularly from untrusted sources, should be considered suspicious.

Example 2: Carlos

ZScaler Report

- “njRAT Pushes Lime Ransomware and Bitcoin Wallet Stealer”
- https://www.zscaler.com/blogs/research/njrat-pushes-lime-ransomware-and-crypto-wallet-grabbers
- Google: njrat zscaler

ZScaler Report

Indicators of Compromise

MD5
dee4b5a99bcd721c3a88ae3180e81cc1
35bd9b51781dfb64fd5396790265ab10
c7dc42db2f7e5e4727c6f61f9eed0758
01b791955f1634d8980e9f6b90f2d4c0

C&C
online2018.duckdns.org
oficinabogota.duckdns.org

ZScaler Report

- Base of the Pyramid
  - Sample hashes
  - Dynamic DNS domains

ZScaler Report

Ransomware functionality

The ransomware encrypts files with the extension **.lime** using the AES-256 symmetric algorithm, which means the key is the same for encryption and decryption.

ZScaler Report

- Base of the Pyramid
  - Sample hashes
  - Dynamic DNS domains
  - Encrypted files are named “.lime”
    - Extend to other ransomware

ZScaler Report

The malware shuts down and restarts the system with the following command:

```
Interaction.Shell("shutdown -r -t 00 -f", AppWinStyle.Hide, false, -1);
```

Switches:

-r -> restart the computer that's currently being used

-t -> time, in seconds

-f -> forces running programs to close without warning

ZScaler Report

- Base of the Pyramid
  - Sample hashes
  - Dynamic DNS domains
  - Encrypted files are named “.lime”
    - Extend to other ransomware
  - Command used to restart machine
- Top of the Pyramid
  - After encrypting files, the machine is restarted

ZScaler Report

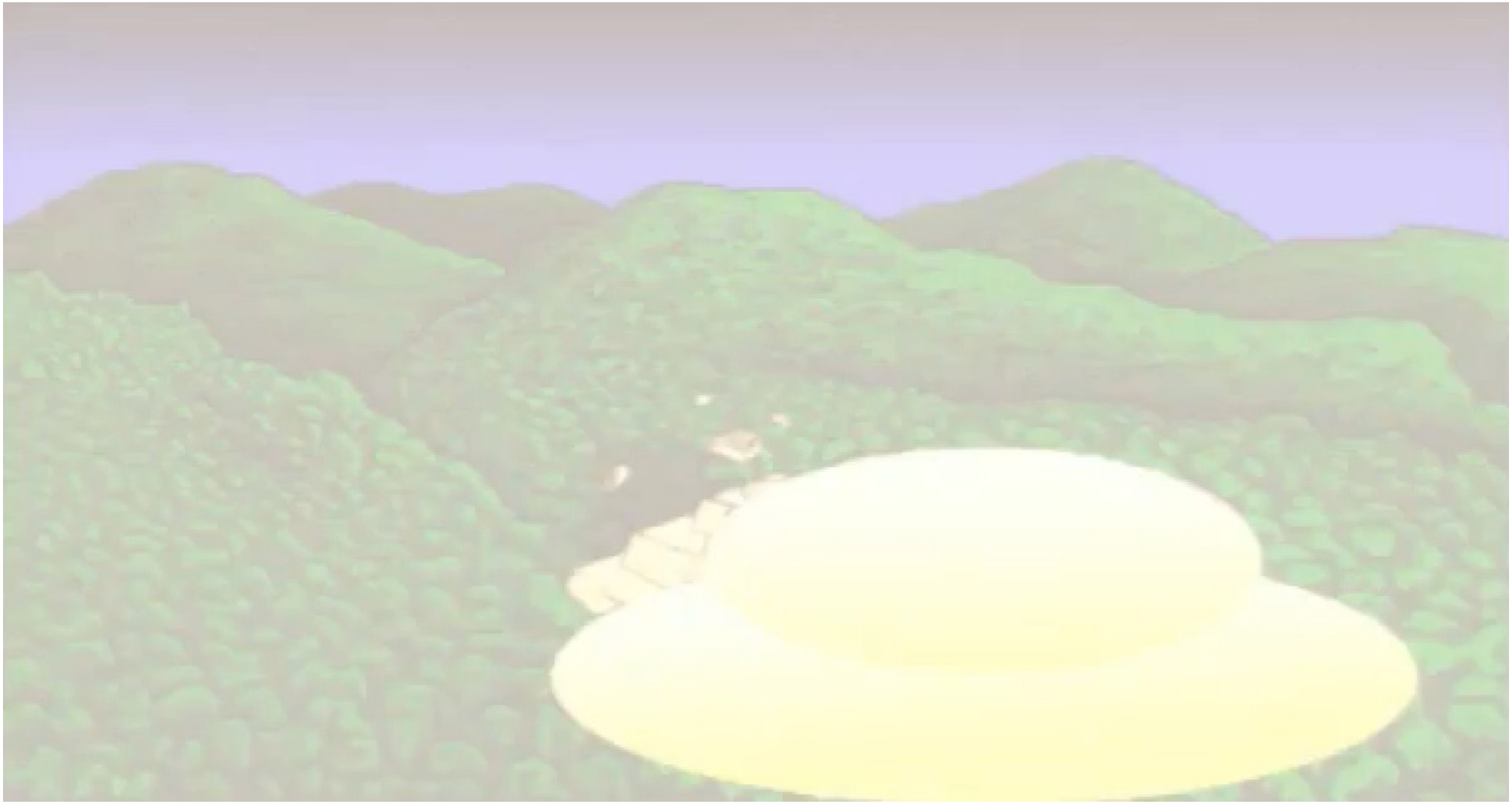
The malware leverages windows WMI queries, such as "SELECT * FROM AntivirusProduct" and "SELECT * FROM Win32_VideoController" to check for VM or sandbox environment.

ZScaler Report

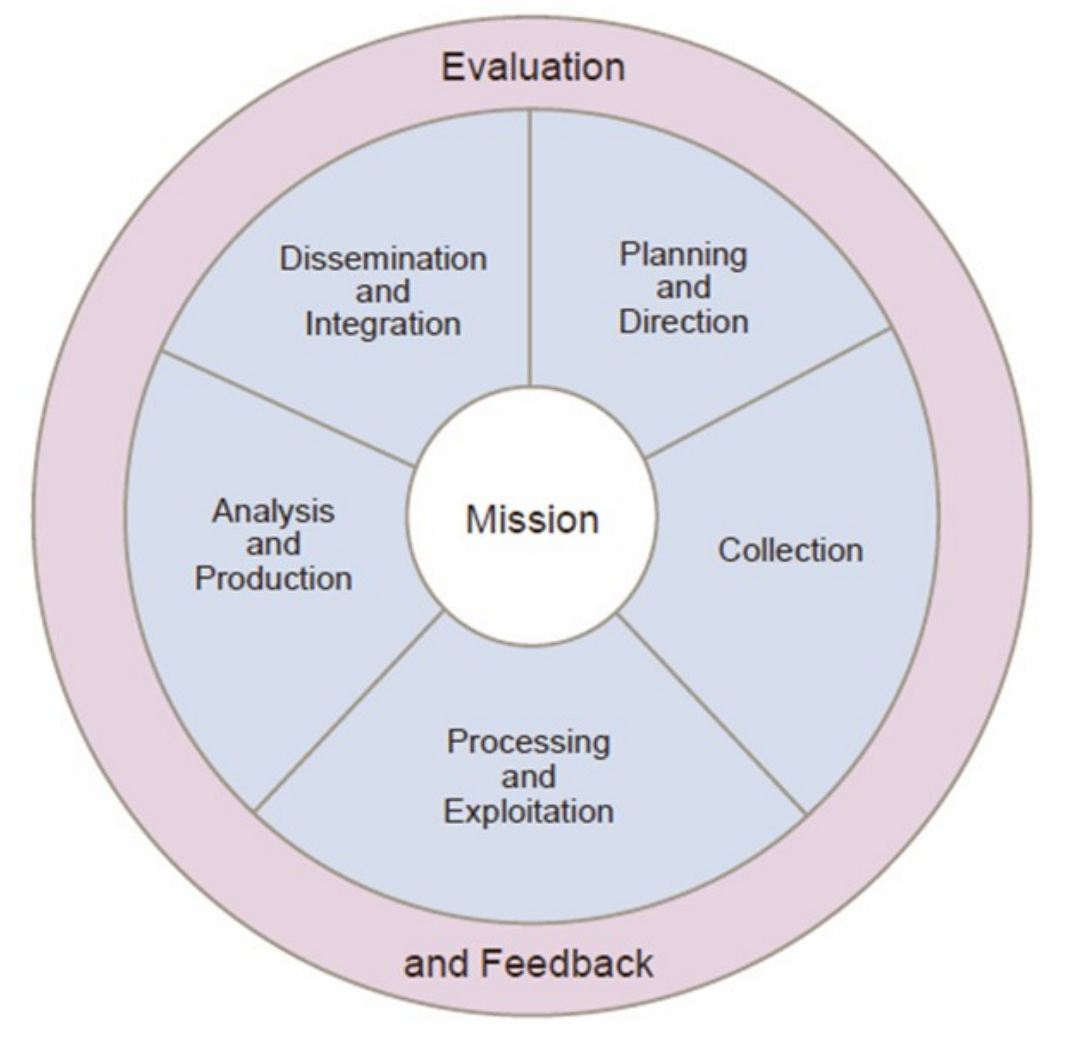
- Base of the Pyramid
  - Sample hashes
  - Dynamic DNS domains
  - Encrypted files are named “.lime”
    - Extend to other ransomware
  - Command used to restart machine
  - Specific WMI queries
- Top of the Pyramid
  - After encrypting files, the machine is restarted
  - Uses WQL to check for a virtualized environment

Parting Thoughts

Parting Thoughts



The Intelligence Cycle



Join Intelligence / Joint Publication 2-0 (Joint Chiefs of Staff)

The Intelligence Cycle

Join Intelligence / Joint Publication 2-0 (Joint Chiefs of Staff)

Keep It Secret, Keep It Safe

- Make time to hunt
- Read the report
- Google it!
- Remember the larger context of an indicator
- Learn regular expressions
  - https://alf.nu/RegexGolf

greetz

- @TryCatchHCF
- @EvilEyeShawn
- My GLE crew