Pathways Into Darkness

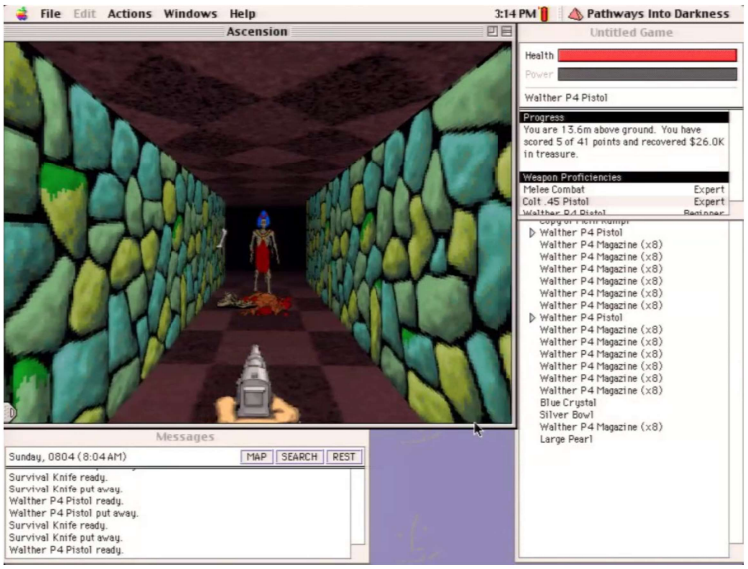
Hunting for Adversary Behaviors Atop The Pyramid Of Pain

Good morning to the audience

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...



So this is Pathways Into Darkness
Pre-Marathon (Pre-Halo) Bunjie game
Deliver a nuke deep within a pyramid to prevent a slumbering god from destroying all the things

Interesting because:
You get a crystal that lets you talk to those that were taken by the pyramid's hazards
- Spanish-speaking conquistadors
- German occultists

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”

Like have been hearing about or dealing with IOCs or “eye-ocks” for some time.

If you see one of these, you think: Oh that’s bad.

IOAs, IOCs, Anemones?

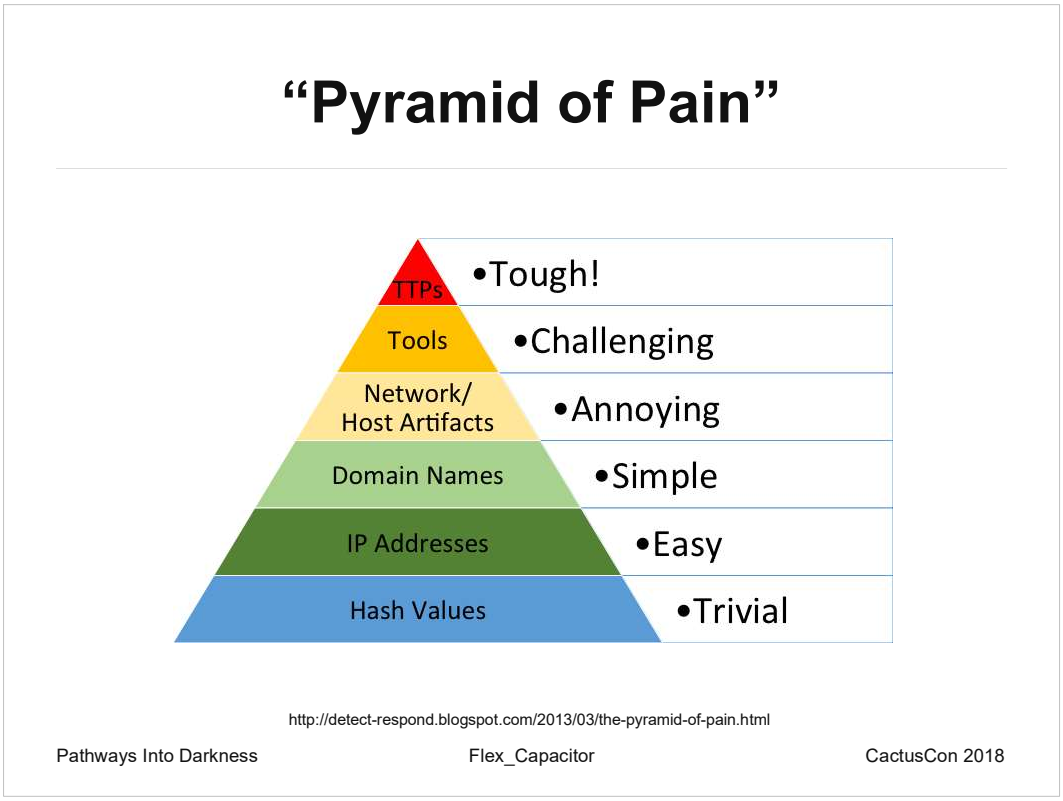
- Indicator of Attack
  - Not concrete, but can lead to earlier detection
  - A launching point for hunting
  - Potentially low fidelity
  - “Huh, That’s Weird”
  - Example:
    - You see a host on your DMZ trying to talk a server used by your product development team to store alpha builds

Often, signs of an attack will be available before a successful intrusion attempt. Can see reconnaissance being conducted by an adversary, or see some network activity that generally makes you think “Huh, that’s weird”

IOAs, IOCs, Anemones?

Joel Carnat / Dutch Grown

These are both Anemones!
Much like “indicators”, it’s a little vague...



Written about back in 2013 by David Bianco

Each level signifies how difficult it is for an actor to respond to mitigations.

Example: If we detect a hash, it's trivial for an actor to get around that.

If we are able to detect customized toolkits, that is much more difficult to adjust to.

A key portion of this model is always remembering that the threat is another human, with their hands on a keyboard, trying to do something to your computers.

Let's briefly go over each of the layers.

Hash Values

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

- calculated based on the contents of a file.
- These are a few different algorithms used to calculate file hashes
- They’re ranked in order of hash value length – shorter means there’s a higher chance that two files will have the same hash – if you really need to know for sure that a file is the same, use a longer one
- “Why is this marked “Trivial”?
  - You only need to change one bit – flip a single one to a zero – to change the entire hash

IP Addresses

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

- Why is this marked “Easy?”
  - An attacker can simply route their connection through another proxy, changing their IP address
  - Akin to changing the return address on an envelope

Domain Names

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

Translated to IP addresses
Why is this marked “Simple”?
An actor needs to only register a new domain name, which takes a minute or two.

Dynamic DNS services simplify this even further – just spin up a subdomain

Distinction between the TTP and the atomic indicator

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

Why is this “annoying”?
This requires some manual effort to work around for an actor: if we’re detecting the naming scheme used by their installer, the tool will stop working
If we’re detecting the user agent string they’re using and silently dropping connections, they need to figure out why the connection dropped and adjust

These are relatively simple to fix for an attacker, but they’re starting to have to put in some actual work.

Tools

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

As we build better capabilities to detect the base of the pyramid, we begin to render out of the box tools far less useful.

Robust AV signatures, well-tuned WAFs, etc all help towards this goal.

Why is this Challenging? An actor would either need to switch techniques or gain much more familiarity with the tools at their disposal to continue to have success.

Tactics, Techniques, Procedures

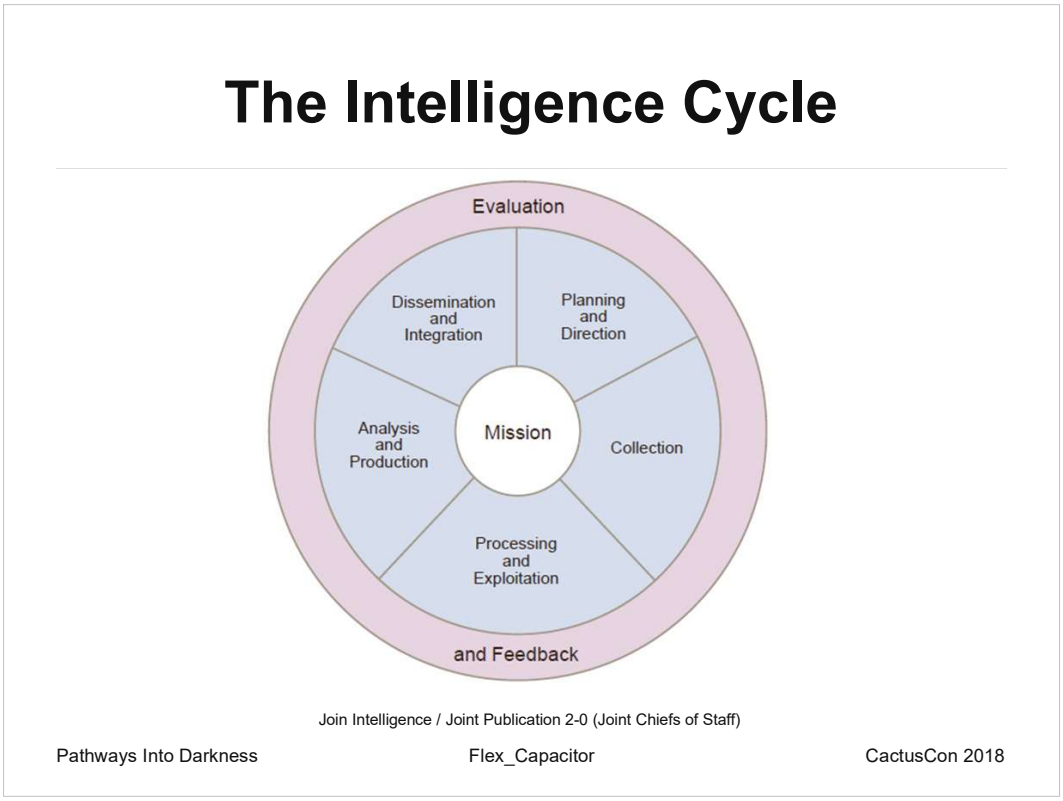
- Example:
  - Spearphishing a target employee, using a malicious PDF that contains a link to an executable disguised as a zip file.
- Example mitigations:
  - Heuristic detection of spearphishing
  - Detecting files whose headers don't match their file extension
  - Detecting network connections initiated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

TTPs: the ways a person carries out an attack

Being capable of detecting and responding at this level is an overarching goal of blue teams.

Rather than affecting the actor's ability to use tools they are familiar with, you are damaging their capability to conduct an operation through the means in which they are comfortable.

This will force an attacker to either up their game, or move on to another target.



Before moving forward, I wanted to review the intelligence cycle for some context.

> Walk through the circle

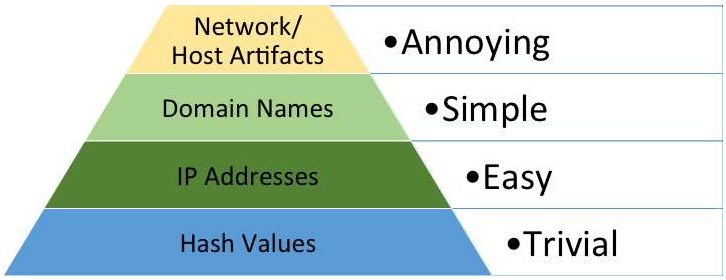
Our sources we collect can be numerous and produce intelligence at a high rate. Intelligence reporting is inevitably a part of every SOC analyst's week, and I wager it will be more prevalent in the future as we begin to automate away some of the work required for the lower tiers of the pyramid.

Challenges SOCs Face

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

- High volume of reporting
  - OSINT
    - Twitter, intel branches of vendors, others
  - Paid
- Limited Resources
  - Headcount/retention issues
  - Budget – tools cost money and/or require maintenance
  - Maybe the tool you have doesn’t do everything you’d want it to do
- Automation can help a lot, but it’s still limited to the lower tiers of the pyramid
- Hunt for Badness
  - Intentionally vague, broad
  - Paralysis of choice or analysis
    Where do I even begin???
  - However, hunting is how we build our capabilities as analysts, and how we start finding activity higher on the pyramid

Base of The Pyramid

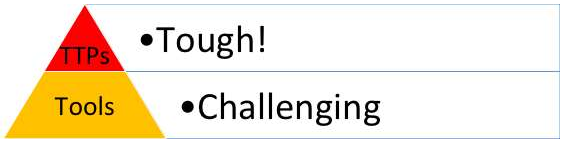


http://detect-respond.blogspot.com/2013/03/the-pyramid-of-pain.html

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

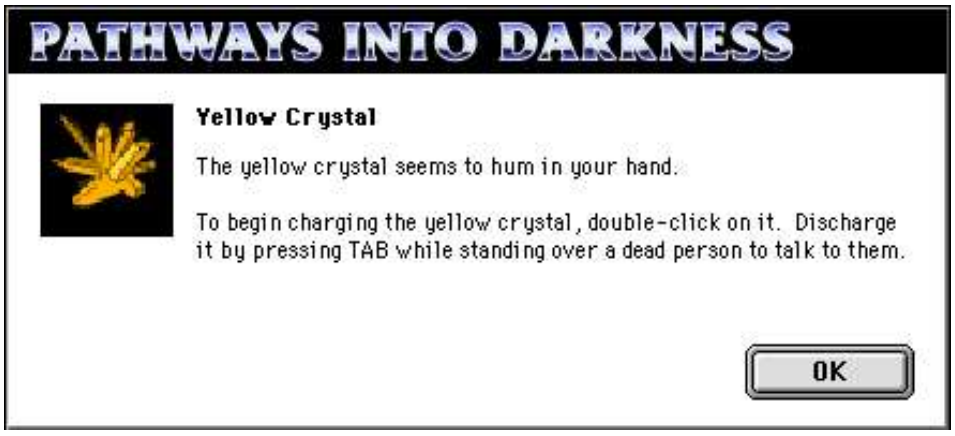
Top of The Pyramid



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

- This still leaves the top of the pyramid! Higher value targets, but require more sweat
- Herein lies an opportunity for hunting, but again, where to begin?

Necroliteracy



Fortunately, we have a Crystal!
People have put forth the effort of documenting post-mortems of APT campaigns and malware analysis!
READ THE REPORT!
You could have a 12-page report with 5 lines of atomic indicators: how do you capture that other analysis?
“Where do I even find that!?”
- I don’t know! But someone in your organization should, and then you will too.
“What if they don’t know either!?”
- A great opportunity to build out your logging!

Reading Strategies

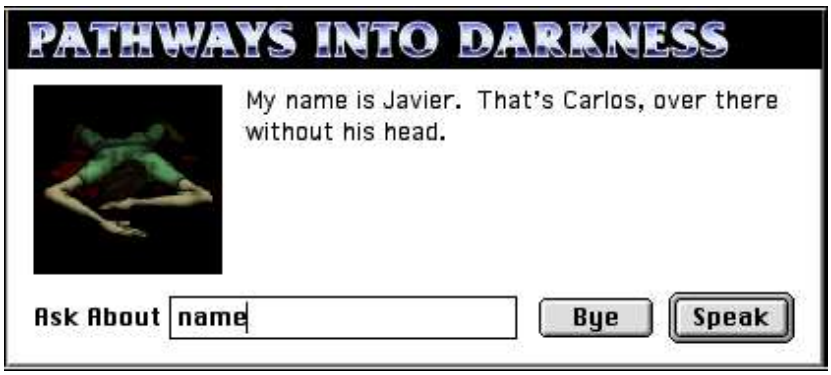
- Try to recognize patterns:
  - Behaviors
  - Naming conventions
  - Subject line flavors
- Understand the attack
- Consider the context
- Think specifically
- Think broadly

Understand – Does the report mention a technology you've never heard of? Google it! Be curious, and take ownership of your learning.

Context – Consider the situation behind the report. Nothing occurs in a vacuum.
Don't need to get into attribution, but:
If a report says Pakistani actors are targeting India, consider the history that drives that interaction.
Consider adversarial relationships in your domain.
Who would want to target you?
How would you modify the techniques used?
Subject line example.

Specific: Find a particular URL scheme
Broad: Find the means by which a sample calls out
For each part of the report, think: how would I find this?

Example 1: Javier



Some reports are incredibly analyst-friendly, like Javier here. Ready to answer our questions!

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 is a network security company that makes detection tools, they got acquired by Gigamon.

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

So here are the indicators, but with some context to go along with them which is nice.

Notice anything?
All of the IOCs are tier 3-6, or what amount to busywork for an adversary to change.

Okay, well that wasn't too exciting, what's in the report?

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

TTP! This is how the c2 URL gets crafted
Tier 1!
But how do we look for that pattern?

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

If you want to learn more, I recommend regex golf
Plenty of resources available online for understanding regular expressions

ICEBRG Report

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

Figure 6: Computation of the stabURL

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

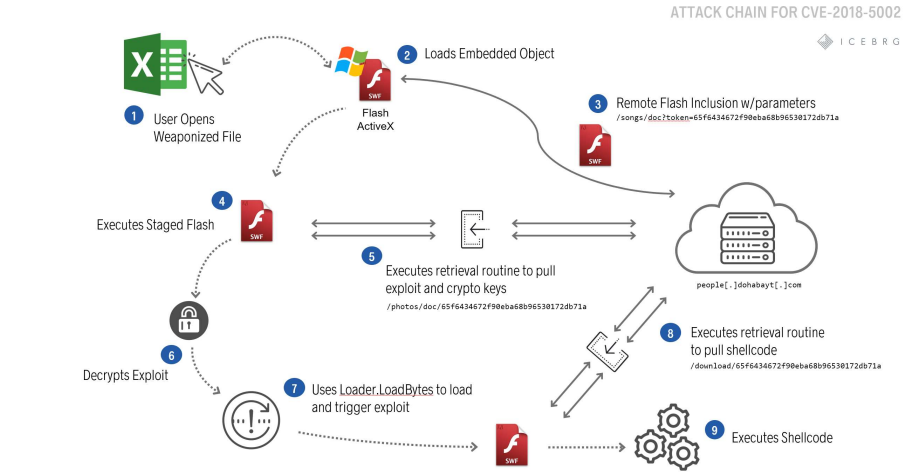
And like that, we’ve built a detection for the c2 that doesn’t focus on the domain or the IP contacted, but the pattern used to craft the URL.

Changing this would require making some changes to the infrastructure as well as the delivery method.

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



Pathways Into Darkness Flex_Capacitor CactusCon 2018

The report also contains this overview of the attack, which nicely highlights other places we might try to look to prevent this kind of attack.

Example:
Excel using activex to talk to something
Activex executing flash

Remember: we're still operating at the top of the pyramid.

Okay, but what about the c2 domain itself?

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?

While it’s not immediately apparent, the domain name is broken up into two parts. Consider the context of this.

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.

Something I really love about this report is it suggests TTPs to look for in plain English alongside the atomic indicators.

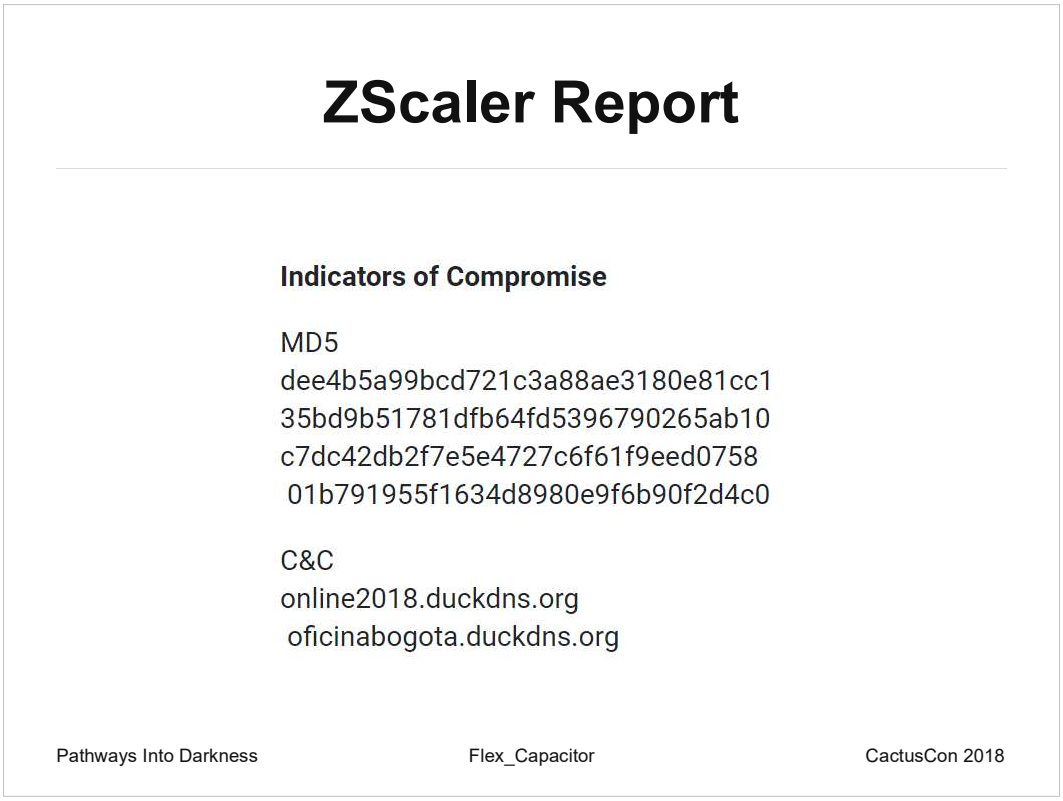
You may not know how to look for these TTPs immediately, but now you have something else to google!

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 is a cloud-based security-as-a-service company.

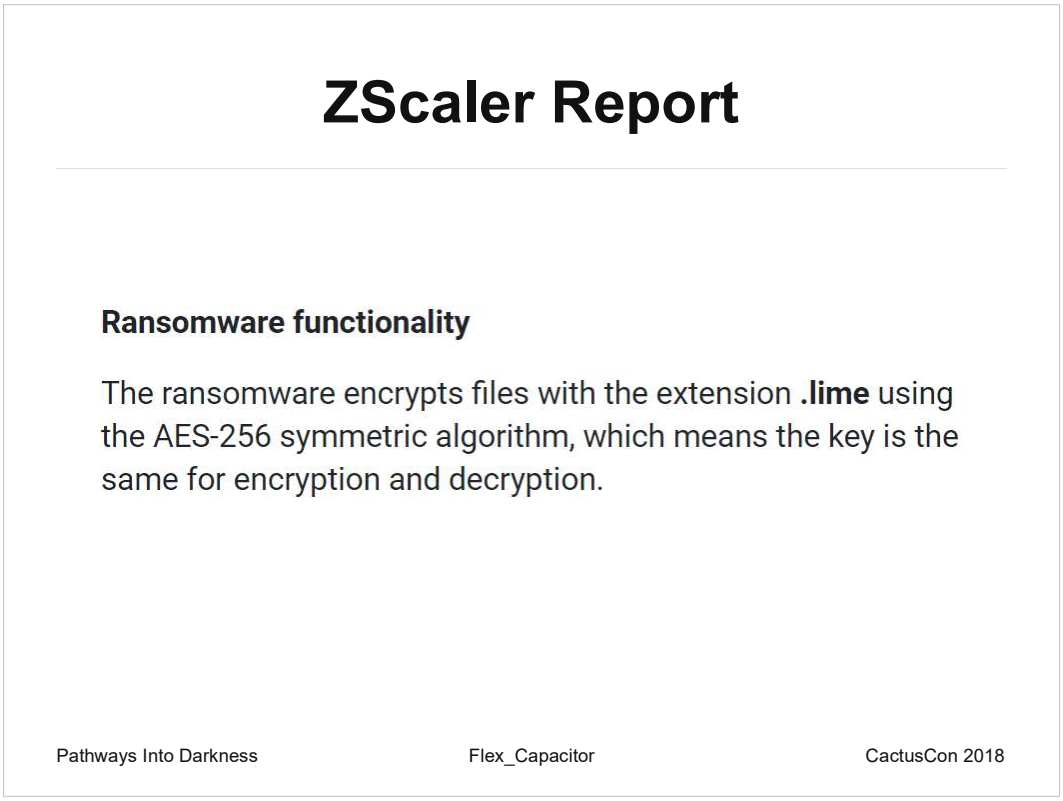


Note again that the IOC section only covers Tiers 3-6. Also, note that the c2 is dynamic dns.

Now, if that's all we have, what can we do?
Block dynamic DNS?
See if we can pull those hashes and do some reversing of our own, but that's not necessarily a skill in everyone's toolkit.

ZScaler Report

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

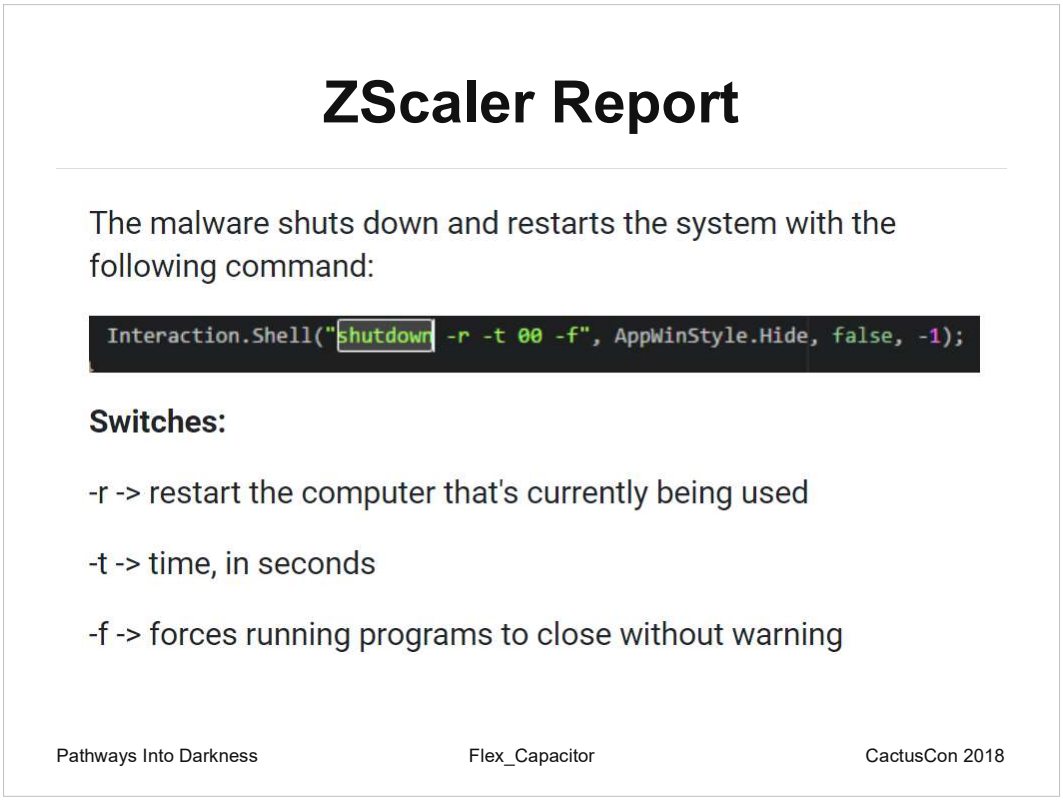


While this is Tier 3, it nonetheless would require a an augmentation of the

What's a jumping off point from here?
Common ransomware extensions!

ZScaler Report

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



Report lays out the behavior (which is interesting enough on its own), and shows the code used. How do we find this?

Interaction.Shell – suggests a cmdline invocation

Look for applications trying to “shutdown”

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.

What is WMI? Windows Management Instrumentation
Incredibly useful for actors who want to “live off the land”, or use readily available tooling from the OS. Also, it gets logged pretty well.

If you don’t recognize those queries, they use WMI Query Language, which is a subset of SQL.

TTPs we’re now hunting for:
VM detection (more advanced behavior)
Interesting WMI queries.

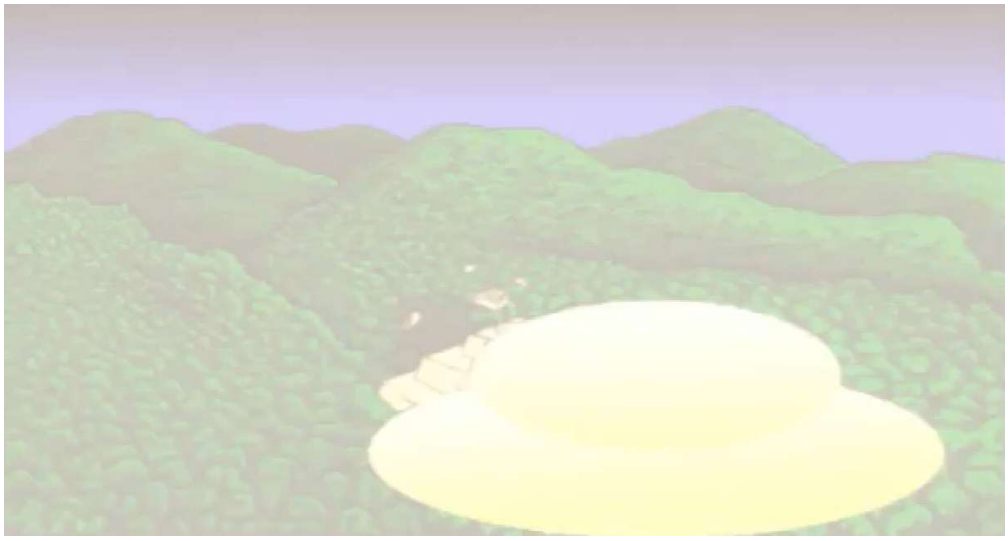
Conveniently for us, there’s a talk right after this about detecting WMI exploitation.

ZScaler Report

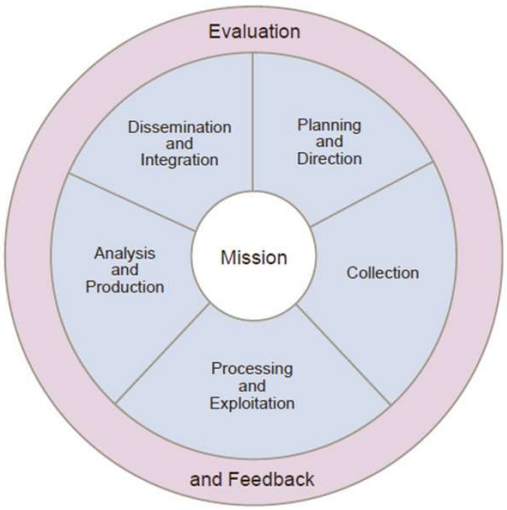
- Base of the Pyramid
  - Sample hashes
  - Dynamic DNS domains
  - Encrypted files are named “.lime”
    - Extend to other ransomware
  - Command used to restart machine
  - Specific WMI queries
- Top of the Pyramid
  - After encrypting files, the machine is restarted
  - Uses WQL to check for a virtualized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

If we assume compromise, then threat hunting is one of the primary means through which you'll detect an actor.

Build out those TTPs from reports into IOA alerting. Taking the time every week or a bit a day might be hard at first, but soon it will be routine and you'll have built up methods and ideas for ad-hoc hunting. See something weird on the wire? Figure it out!

Even if it turns out to be benign, it's a great way to learn your environment, and you'll have built understanding.

greetz

- @TryCatchHCF
- @EvilEyeShawn
- My GLE crew