mWISE™
MANDIANT WORLDWIDE
INFORMATION SECURITY EXCHANGE

QUACK ~~Cracking~~ the Beacon: Automating the extraction of implant configurations

Derek Ditch

Principal Security Research Engineer
Elastic

Jessica David

Senior Data Engineer
Elastic

Agenda

- Background
- Malduck & Configuration Extraction
- Quacking the Code & Demo
- Future Work

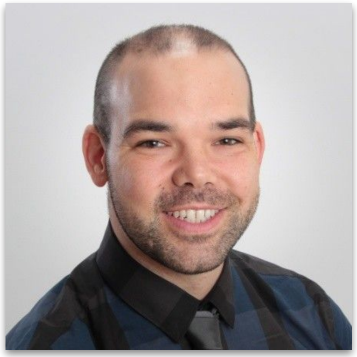
elastic

mWISE

Who are we?

Derek Ditch (he/him)

- Works on team of threat researchers at Elastic
- Background in Intel Community, Network Forensics, and Malware Analysis
- 22 year veteran of Missouri National Guard, Cyber Team
- Lives in TX with wife, 4 kids, 2 dogs, and a cat



Who are we?

Jessica David (she/her)

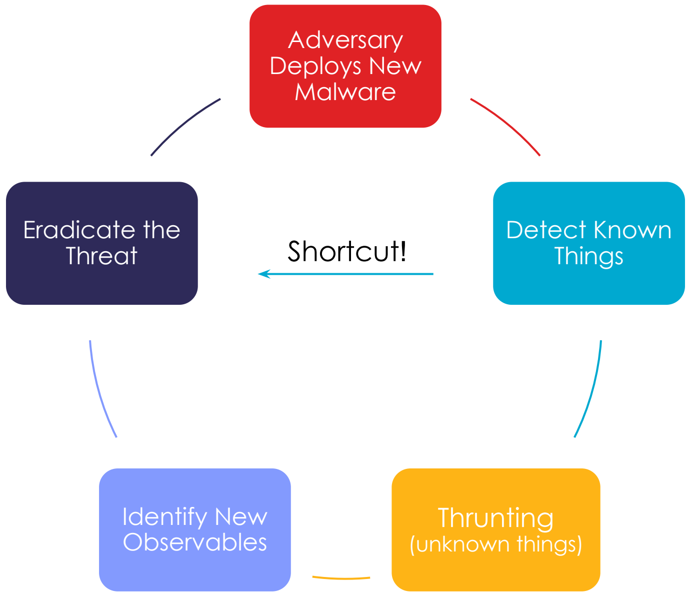
- Works on team of software engineers that build the cloud services & data systems that help users find and understand the threats facing their organizations
- Career data pusher (Microsoft SQL, IBM Netezza, Hadoop, etc)
- Devoted cat mom
- Amateur woodworker

mWISE™
MANDIANT WORLDWIDE
INFORMATION SECURITY EXCHANGE

Adventures of Analysis

Our Motivation

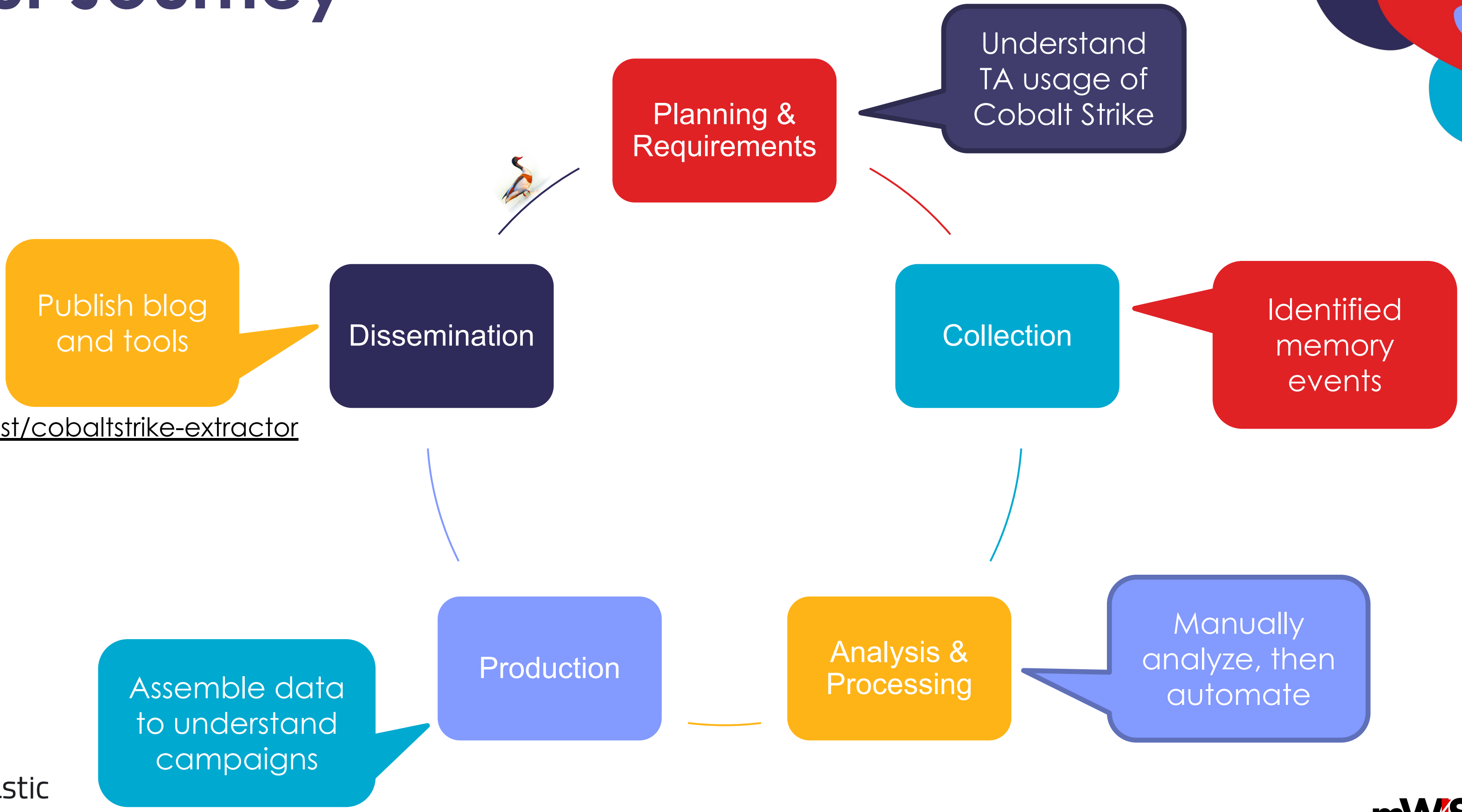
Stop fighting in the trenches



The Starting Idea

1. Take a bunch of Cobalt Strike samples
2. Extract beacon configs
3. Store them in a standardized way
4. Run automated detections

Our Journey



ela.st/cobaltstrike-extractor

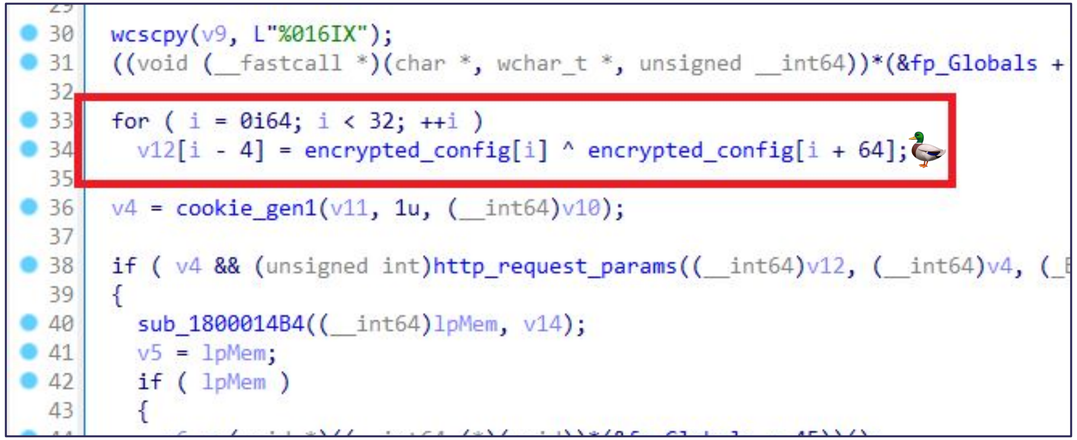
🦆 Enter Malduck 🦆

- Malduck is a powerful static malware analysis tool created by CERT Polska*
- Provides powerful config extraction of malware features using YARA rules + Python
- So, find malware, dump it into a processing pipeline, find C2 and other information much faster than the manual process

★ Special thanks to @c3rb3ru5d3d53c for her awesome contributions with mwcfg

Extraction Workflow (IcedID)

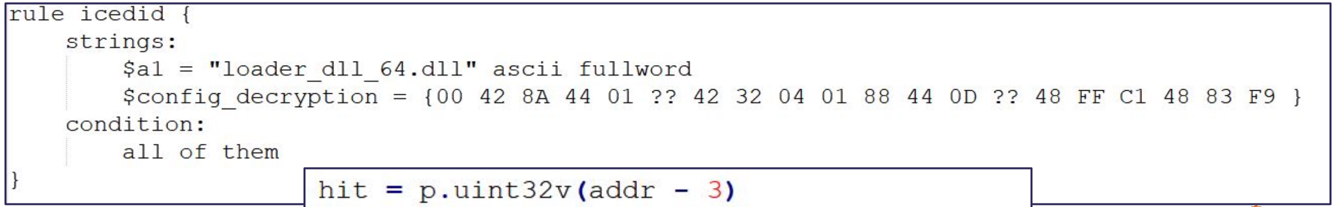
Identify key functions in malware (encryption/decryption)



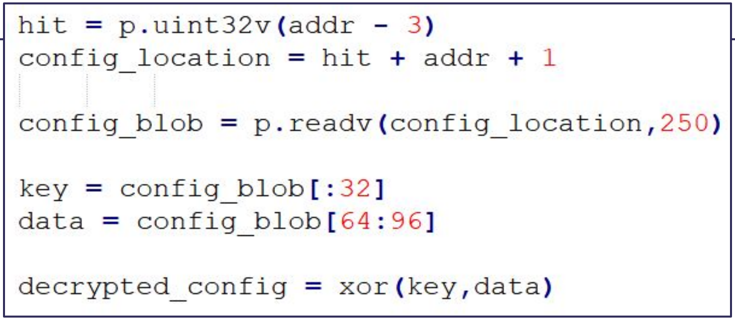
```
wcscpy(v9, L"%016IX");
((void (__fastcall *)(char *, wchar_t *, unsigned __int64))*(&fp_Globals +

for ( i = 0i64; i < 32; ++i )
  v12[i - 4] = encrypted_config[i] ^ encrypted_config[i + 64];

v4 = cookie_gen1(v11, 1u, (__int64)v10);

if ( v4 && (unsigned int)http_request_params((__int64)v12, (__int64)v4, (_
{
  sub_1800014B4((__int64)lpMem, v14);
  v5 = lpMem;
  if ( lpMem )
  {
```

Extraction Workflow (IcedID)

Generate YARA rule to pull in offset address of function and registers/values nearby



```
rule icedid {
    strings:
        $a1 = "loader_dll_64.dll" ascii fullword
        $config_decryption = {00 42 8A 44 01 ?? 42 32 04 01 88 44 0D ?? 48 FF C1 48 83 F9 }
    condition:
        all of them
}
```



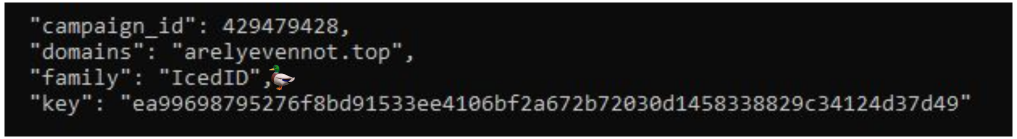
```
hit = p.uint32v(addr - 3)
config_location = hit + addr + 1

config_blob = p.readv(config_location,250)

key = config_blob[:32]
data = config_blob[64:96]

decrypted_config = xor(key,data)
```

elastic

mWISE |

Extraction Workflow (IcedID)

Write some Python to capture critical data



```
"campaign_id": 429479428,
"domains": "arelyevennot.top",
"family": "IcedID",🦆
"key": "ea99698795276f8bd91533ee4106bf2a672b72030d1458338829c34124d37d49"
```

We need samples

We've got some options:

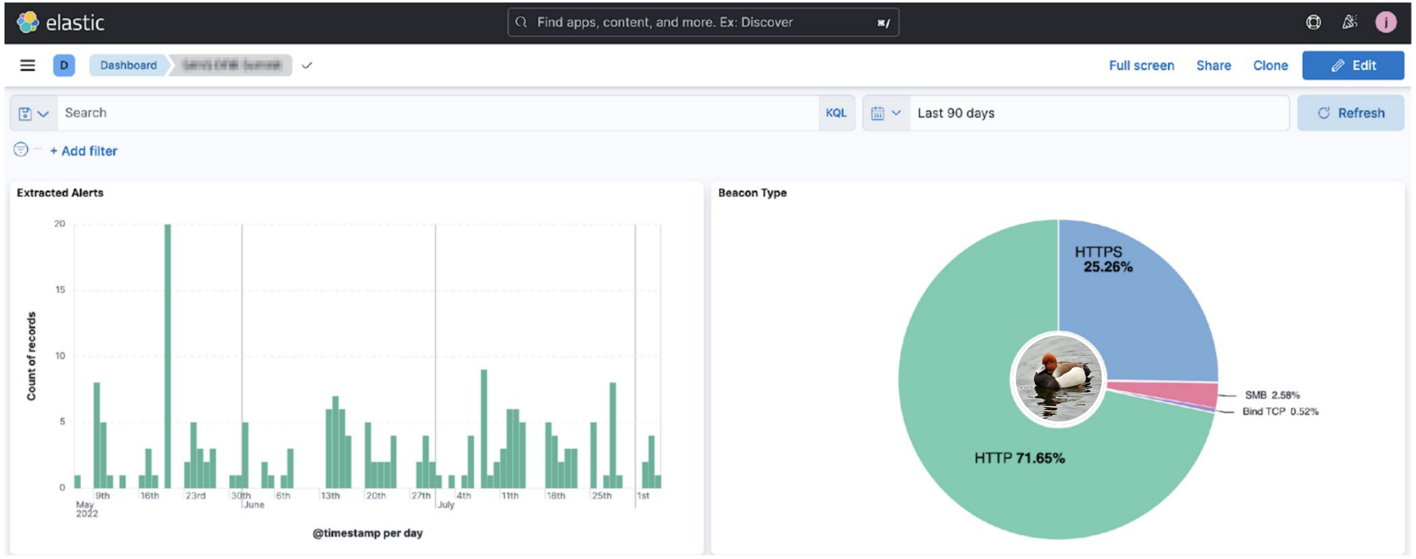
- We can analyze malware statically on disk (if it's written to disk)
- We can analyze memory captures
  (don't worry, it won't hurt)

Quacking the Code

Stop. "Demo" Time!

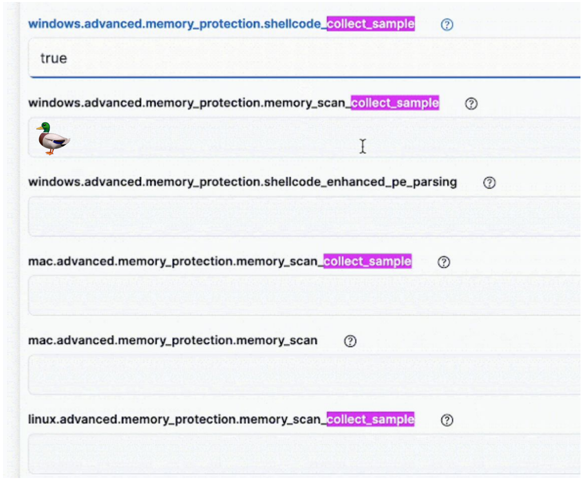
How It Works

- Run a daily batch job against endpoint alerts
- Extract & load enhanced alerts into a searchable index



About Exquacking

- Pulls Endpoint alert data from endpoint security
  - We use Elastic, but you can use your favorite tool!
- Requires an endpoint policy configured with sample collection, e.g.:



windows.advanced.memory_protection.shellcode_collect_sample
true

windows.advanced.memory_protection.memory_scan_collect_sample
🦆

windows.advanced.memory_protection.shellcode_enhanced_pe_parsing

mac.advanced.memory_protection.memory_scan_collect_sample

mac.advanced.memory_protection.memory_scan

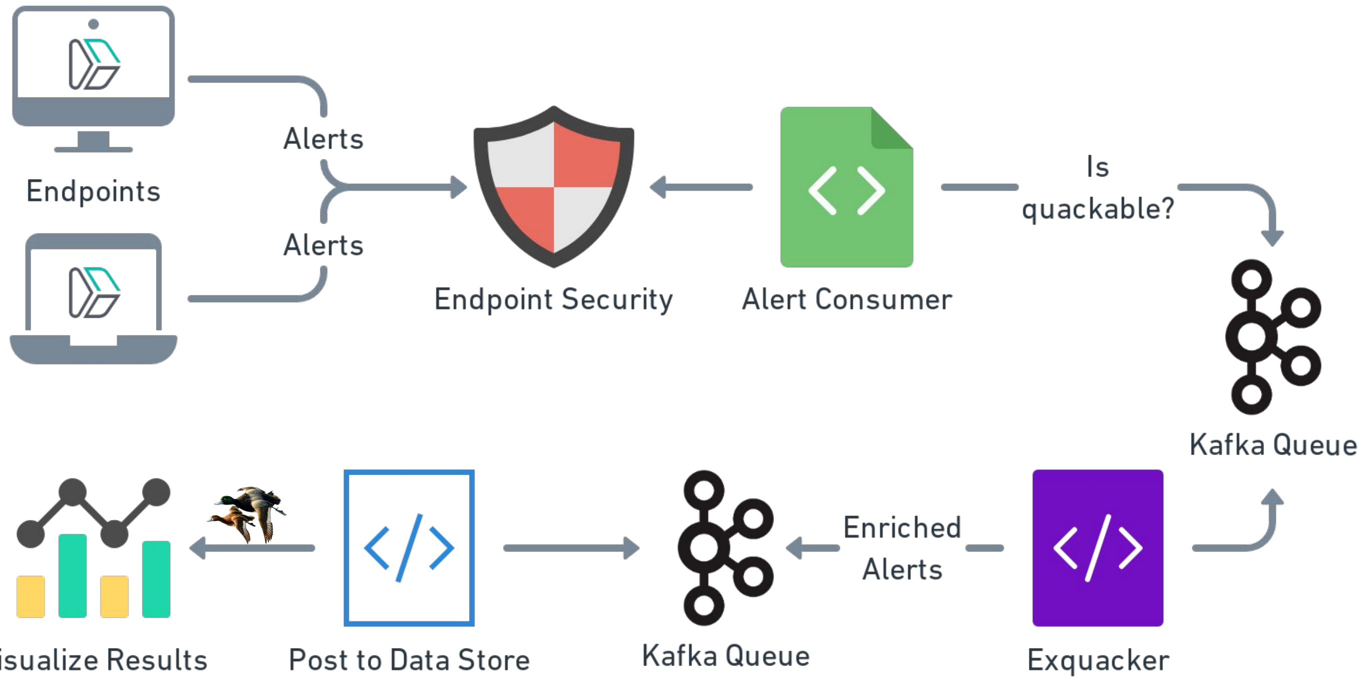
linux.advanced.memory_protection.memory_scan_collect_sample

elastic

mWISE |

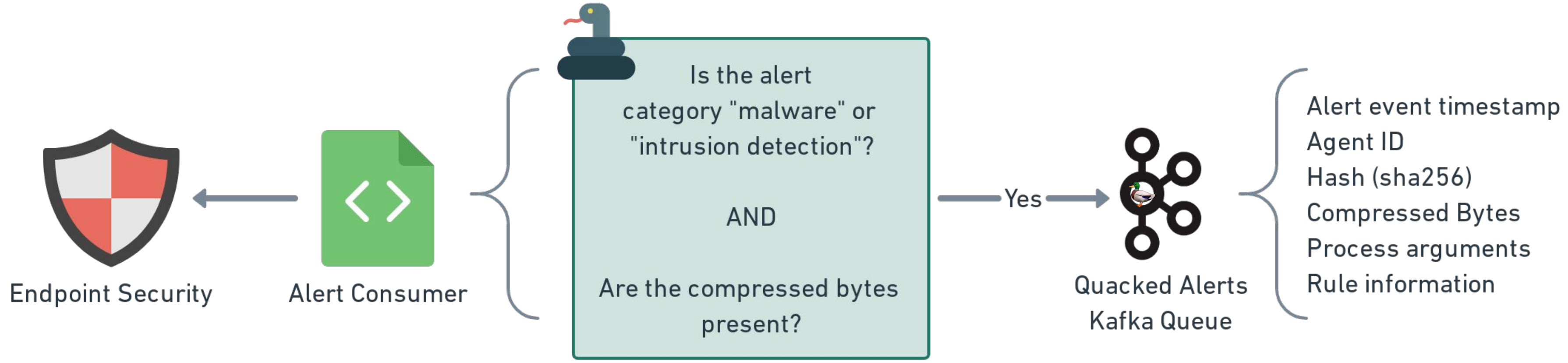
Next Step: make it faster!

Near real-time with consumers & queues



elastic

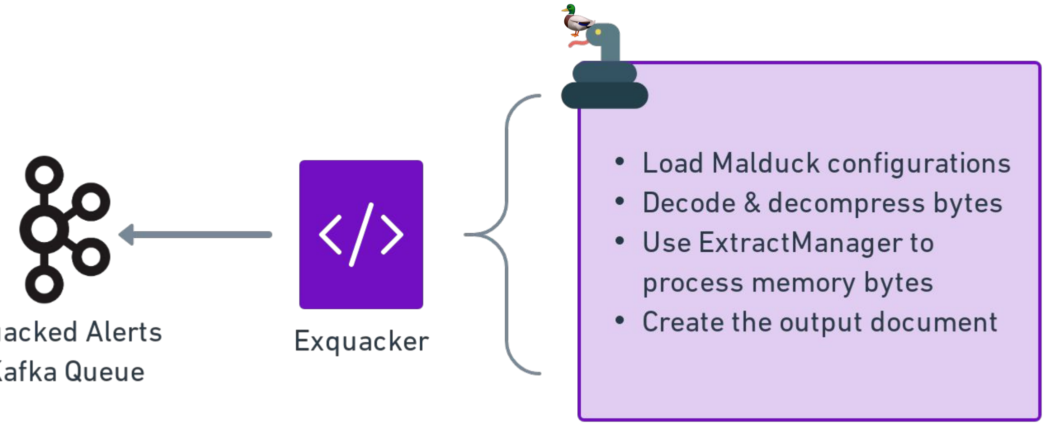
What makes it “quackable”?



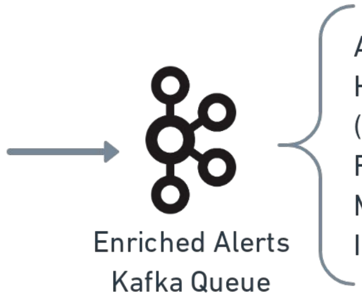
elastic

mWISE

How We Enrich Alerts

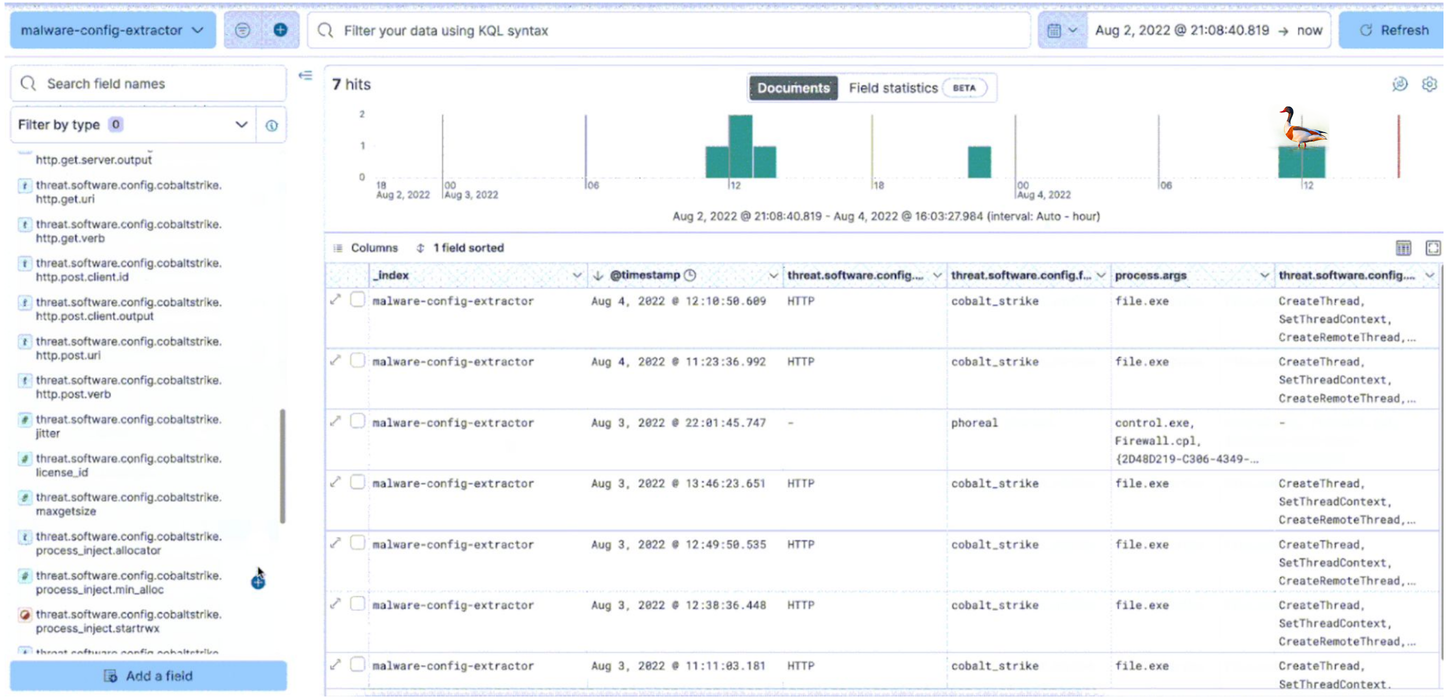


- Load Malduck configurations
- Decode & decompress bytes
- Use ExtractManager to process memory bytes
- Create the output document



Alert event timestamp
Hash (sha256) and details (name and size)
Rule information
Malware family
Info gained from exquacking

Sample Data



http.get.server.output
threat.software.config.cobaltstrike.http.get.uri
threat.software.config.cobaltstrike.http.get.verb
threat.software.config.cobaltstrike.http.post.client.id
threat.software.config.cobaltstrike.http.post.client.output
threat.software.config.cobaltstrike.http.post.uri
threat.software.config.cobaltstrike.http.post.verb
threat.software.config.cobaltstrike.jitter
threat.software.config.cobaltstrike.license_id
threat.software.config.cobaltstrike.maxgetsize
threat.software.config.cobaltstrike.process_inject.allocator
threat.software.config.cobaltstrike.process_inject.min_alloc
threat.software.config.cobaltstrike.process_inject.startrwx

7 hits

Aug 2, 2022 @ 21:08:40.819 - Aug 4, 2022 @ 16:03:27.984 (interval: Auto - hour)

Columns 1 field sorted

_index	@timestamp	threat.software.config....	threat.software.config.f...	process.args	threat.software.config....
malware-config-extractor	Aug 4, 2022 @ 12:10:50.609	HTTP	cobalt_strike	file.exe	CreateThread, SetThreadContext, CreateRemoteThread,...
malware-config-extractor	Aug 4, 2022 @ 11:23:36.992	HTTP	cobalt_strike	file.exe	CreateThread, SetThreadContext, CreateRemoteThread,...
malware-config-extractor	Aug 3, 2022 @ 22:01:45.747	-	phoreal	control.exe, Firewall.cpl, {2D48D219-C306-4349-...	-
malware-config-extractor	Aug 3, 2022 @ 13:46:23.651	HTTP	cobalt_strike	file.exe	CreateThread, SetThreadContext, CreateRemoteThread,...
malware-config-extractor	Aug 3, 2022 @ 12:49:50.535	HTTP	cobalt_strike	file.exe	CreateThread, SetThreadContext, CreateRemoteThread,...
malware-config-extractor	Aug 3, 2022 @ 12:38:36.448	HTTP	cobalt_strike	file.exe	CreateThread, SetThreadContext, CreateRemoteThread,...
malware-config-extractor	Aug 3, 2022 @ 11:11:03.181	HTTP	cobalt_strike	file.exe	CreateThread, SetThreadContext.

elastic

MANDIANT WORLDWIDE
INFORMATION SECURITY EXCHANGE

Future Work

Where are we headed?

- Continue to automate and publish intel

  https://ela.st/security-labs

- Build more malduck modules and share to community
- Publish Kibana Alerting and Dashboards
- Get community feedback and contributions!

  https://ela.st/malware-exquacker

elastic

mWISE

mWISE™
MANDIANT WORLDWIDE
INFORMATION SECURITY EXCHANGE

🦆 QUACK ~~Thanks~~!

Talk Repo: https://ela.st/mwise-2022

All the links and more ☝️

Derek Ditch

@dcode | in @dditch

Jessica David

@jeska | in @jeska28

mWISE™

MANDIANT WORLDWIDE
INFORMATION SECURITY EXCHANGE