CyShrike

A Bioinformatic Approach to Malware Detection and Forensics

MOSAICS Industry Day Nov 05, 2020

MOSAICS
2020
INDUSTRY
DAY

Cynalytica

Agenda

- CyShrike tool (malware identification and forensics)
- Current attempted malware attack against Oil & Gas industry
- Initial findings
- Benefits of tool
- How it fits into MOSAICS objectives

CyShrike™ - The Bioinformatic Approach

1. CyShrike uses a bioinformatic approach to malware detection by applying ‘Species Concepts’ to the evolution of computer code.

2. Modeled on the biological principle that a species descends from a common ancestor, CyShrike learns the evolutionary relationships among sequences of code and discovers malicious threats by identifying common hereditary traits in their genetic makeup (chains).

3. Unlike conventional and rule-based malware detection tools, CyShrike does not need to store every possible variant of malware code to make its determinations.

4. Instead, it identifies evolving, unseen malware patterns using its unique ability to find similarities between code sequences.

MOSAICS
2020
INDUSTRY
DAY

Cynalytica

USD STP&E: Resilient Systems

"The STP&E Resilient Systems (RS) Directorate focuses on policy and practice to ensure DoD systems are resilient to advanced cyber threats."

Objectives include:

a) Lead program protection planning and system security engineering policy and practices to mitigate the compromise and exploitation of advanced warfighting capabilities

b) Mitigate malicious and non-malicious activity to mission-critical hardware and software in DoD weapon systems

c) Safeguard DoD-controlled technical information from exploitation through cost-effective countermeasures

USD STP&E Resilient Systems Directorate, 2020

MOSAICS
2020
INDUSTRY
DAY

Cynalytica

Evolution of CyShrike

1. Early concept while working with UC Berkeley Center for Information Research for the Interest of Society (CITRIS) on efficiency of surveillance related technology in 2008.

2. Commonality in analysis approach by Ph.D. researchers in development of PCR Technology for cancer research

3. Desire to evolve the idea of a CyberCDC for code to protect Government and Municipalities assets.

4. Functional MVP Prototype June 2020

CYSHRIKE

Evolving Malware Threat

1. Signature-based anti-malware providers need to hold signatures for all possible variants of malware; thus, polymorphic malware renders signature-based anti-malware tools ineffective.

2. Malware authors are using techniques that change malware signatures every time they replicate and infect a new file (Polymorphic Malware) in order to evade detection by conventional, signature-based anti-malware tools.

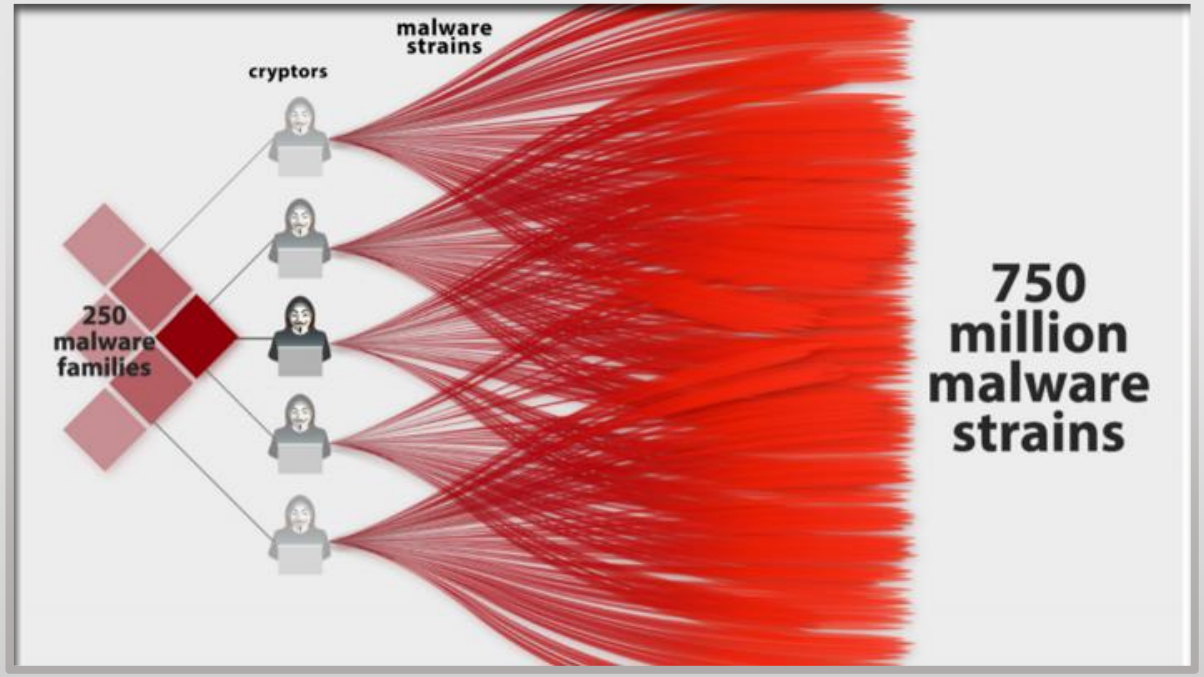
3. The polymorphic malware threat continues to increase in intensity, with recent research from Webroot showing more than 95% of all malicious executables they encounter are polymorphic.

Polymorphic Malware Evades Traditional A/V

1. Easy to evade signature-based tools using mutation engine small alteration will change signature/hash but not functionality

2. ~95% of Encountered Malware is Polymorphic[1,2]

3. Malware is primarily adapted from existing attack families



[1]Microsoft, 2018

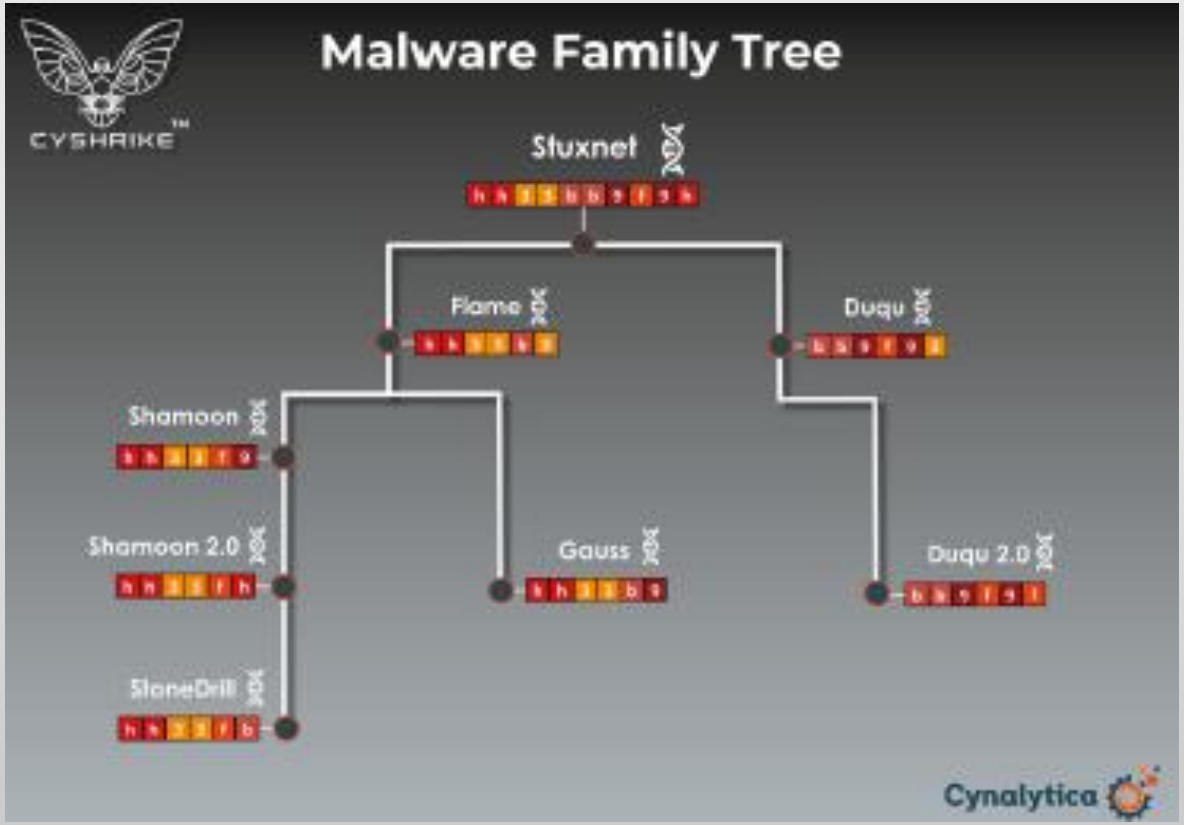
[2]Webroot, 2020

CYSHRIKE

MOSAICS
2020
INDUSTRY
DAY

Cynalytica

Finds Similarities to Known Malware Families



1. **Collection –** Hunter/Gatherer ICS malware
2. **File Breakdown –** Scanned suspect files are broken down into genetic chains
3. **Familial Ties** – Chains compared to database of known-good/bad
4. **Threat Assessment –** Areas of similarity shown for forensic analysis

CYSHRIKE

MOSAICS
2020
INDUSTRY
DAY

Cynalytica

“ Laertes/Odysseus”

“In early 2020, ONE Gas identified malicious code mid stage cycle attempting to download software to provide a live foothold along with profiling users within the Active Directory. Upon detection, this system was immediately powered off due to prior activity already have taken place. The system was imaged and then dissected at a base layer to develop some basic TTPs to determine if further activity resided in the environment. Deeper forensics was not initially available even with leading sandboxing and malware code mapping technology, so I placed my deconstructing on pause when our ongoing strategic partnership with Cynalytica provided a better technology path.”

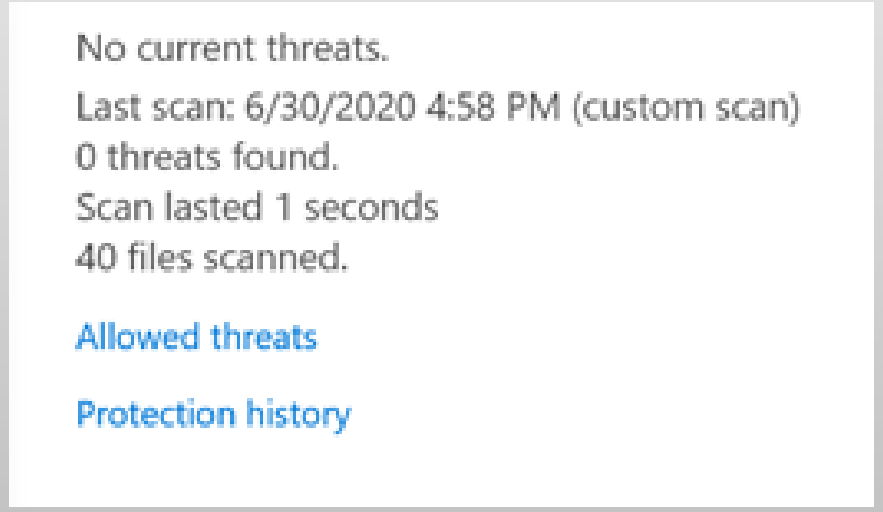
CYSHRIKE

MOSAICS
2020
INDUSTRY
DAY

Cynalytica

“ Laertes/Odysseus”

1. End of June 2020 Capabilities Review with ONE Gas
2. Recent machine quarantined for undetermined A/V hit
3. ONE Gas provide a folder from quarantined machine for CyShrike Analysis
4. Scanned files in folder (No A/V hits)

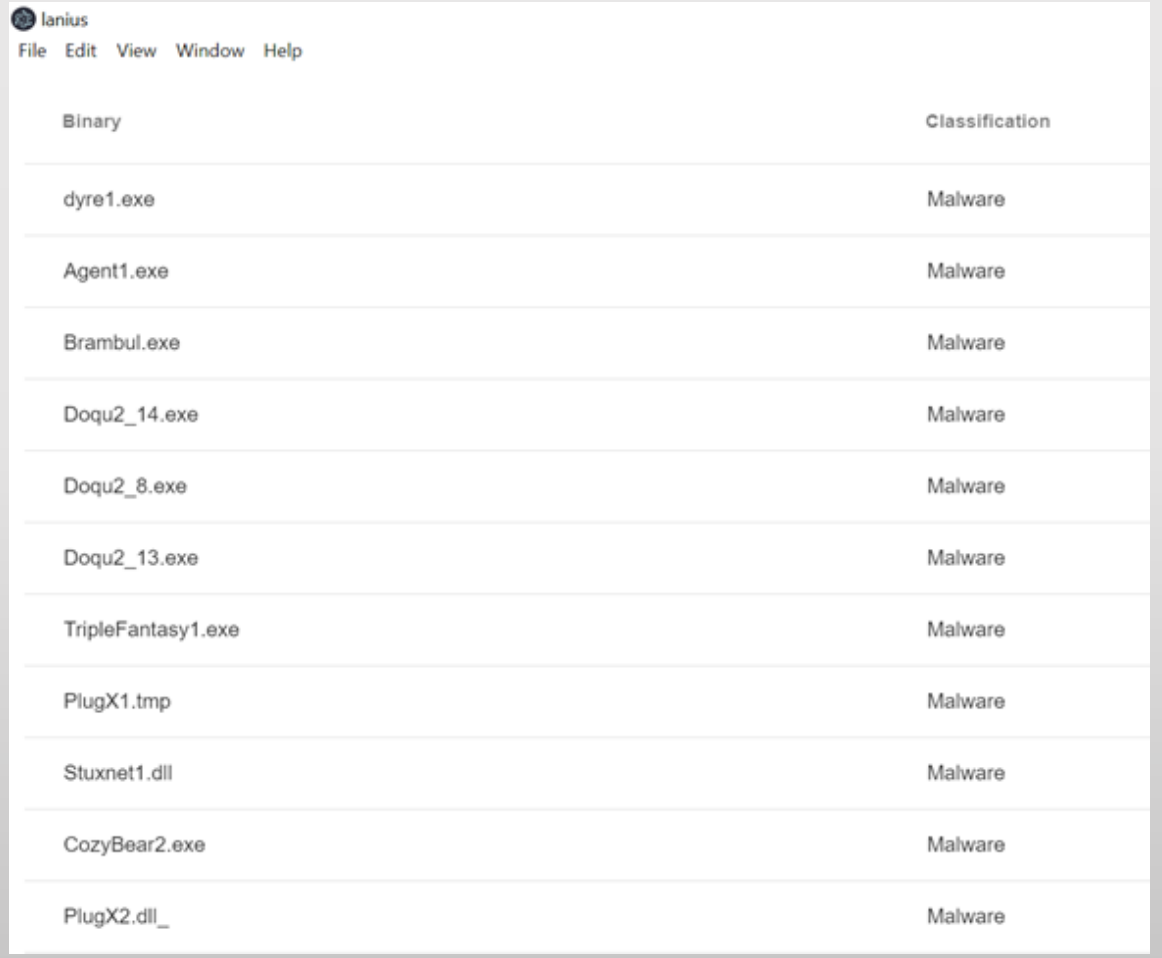


MOSAICS
2020
INDUSTRY
DAY

“ Laertes/Odysseus” – initial hits

Cynalytica

- Brambul
- CozyBear
- CryptoLocker
- Duqu
- GrandCrypt
- GrayFish
- MiniDuke
- Muldrop
- Drye
- Stuxnet
- WannaCry
- TripleFantasy
- And more…



MOSAICS
2020
INDUSTRY
DAY

Cynalytica

“ Laertes/Odysseus”

1. Focused in on ICS malware components

2. Stuxnet matched over 50 common function blocks

3. Leveraging the Windows kernel32.dll API calls
   VirtualAlloc & VirtualFree as malicious injection points

4. Clear picture of breadth of Trojan attack (posing as legitimate files)

5. Sophisticated intent and capability
   a) Create new SIDS
   b) Passwords
   c) Change Firewall and Registry Rules

6. Sophisticated ability to identify and evade and adapt

CYSHRIKE

MOSAICS
2020
INDUSTRY
DAY

Cynalytica

“ Laertes/Odysseus”

1. Other shared malware capabilities including:
   a) Credential Harvesting malware (Banking and Finance)
   b) Ransomware
   c) ICS environment enumeration

2. Common tactics to campaign against Electric Utilities
   Industroyer

3. Matches to malware associated to:
   a) CozyBear
   b) FancyBear
   c) VoodooBear

MOSAICS
2020
INDUSTRY
DAY

Cynalytica

“ Laertes/Odysseus”

1. Pivot to static and behavioural analysis
2. ONE Gas environment well architected to protect against campaign
3. Not all companies as well architected and prepared
4. Hallmarks of a sophisticated actor
   a) Evasion
   b) Monitor
   c) Enumeration
   d) Validate
   e) Morph
   f) Prepare for persistence

CYSHRIKE

MOSAICS
2020
INDUSTRY
DAY

Cynalytica

“ Laertes/Odysseus”

1. Initial High Level Assessment
   a) Very good at validation and enumerating monitoring tools and configurations
   b) Use of undocumented OS functions and calls
   c) Enumeration of users, user contacts and relationships and users calender
   d) Understood local/regional environments and attempted activities in off hour, schedule shifts and vacation/holidays.

MOSAICS
2020
INDUSTRY
DAY

Cynalytica

ONE Gas perspective of CyShrike Capability

1. Tools benefits were
   a) That it took only hours or minutes depending on the sample size to determine malware chain mapping.
   b) Had a heavy OT context, other genetic mapping has some but not all malware families.
   c) Great for basic and complex malware families and code reuse as well!
   d) Provided a Quick output of the overall picture without having an interpreter to tell you what each code family means (reporting and overview)

CYSHRIKE

MOSAICS
2020
INDUSTRY
DAY

Cynalytica

TRL and Contract Path

1. Right now we would classify CyShrike at a TRL6
   a) “Engineering/pilot-scale, similar (prototypical) system validation in relevant environment(s) (ONE Gas and EPRI).
   b) We are still working with industries in the market to build on the corpus of data and verification of associated intelligence and attribution data. We would like to work with DoD and/or DOE to do this.

2. There is no defined contract path to date.

CYSHRIKE

MOSAICS

2020 INDUSTRY DAY

Cynalytica

Technology Validated in Energy Environment

1. Real-World ICS Campaign Analysis
   a) Validation Partners
      i. ONE Gas, Inc.
      ii. Electric Power Research Institute (EPRI)
   b) Methodological similarities between Natural Gas campaign and Industroyer and Stuxnet

2. CyShrike used to focus forensic process and inform response

CYSHRIKE

MOSAICS
2020
INDUSTRY
DAY

Cynalytica

Benefits/Value Proposition(s)

1. Uses a bioinformatic approach to detect malware that constantly changes to avoid detection by identifying common hereditary traits of evolving malicious code.

2. Identifies identical/similar functions or “GENES” between known and new / Zero Days variants of malware that a signature-based anti-malware engine would not detect.

3. Does not require storage of every possible variant of malware code.

4. Does not need: signatures, hashes, strings, or rules to make its determinations, CyShrike can avoid hash obfuscation techniques like spoofing MD5 hashes.

5. Provides detailed visual information on what functions or “GENES” it considers malicious, and where to start a forensic search.

6. CyShrike not only provides malicious determinations, but it also provides analysis of why a file is benign based on functions or “GENES”.

7. Shortens the CVE and incident response process by describing malicious functions that static analysis would take considerable amounts of time to initially discover.

MOSAICS 2020 INDUSTRY DAY

Cynalytica

Enhances Resiliency of Cyber Systems Fills MOSAICS Objective (Malware Detection)

1. **Detect**

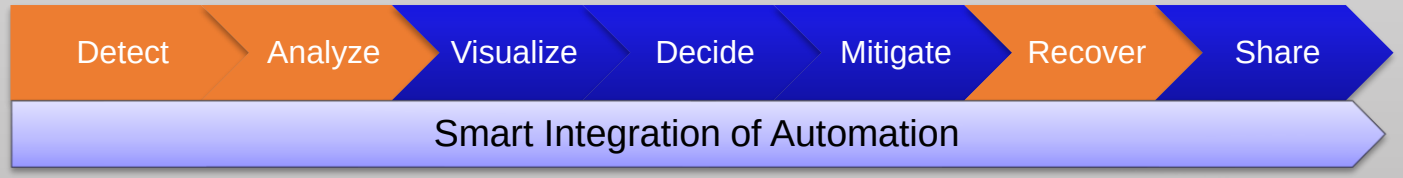
   Suspect files scanned with CyShrike classified as malicious or benign

2. **Analyze**

   Reduced Discovery Time (MTTD) and Analysis Time help limit damage

3. **Recover**

   Targeted forensic capabilities allow operators to pinpoint malicious actions undertaken, making necessary recovery actions clearer



CYSHRIKE

THANK YOU

Richard Robinson
richard@cynalytica.com

Cynalytica