



The Threats Are Changing,
So Are We.

October 2019



About Me

- Five years as CIO in private industry
- Thirty years at the European Commission
 - IT management
 - Internal and external audit
 - COO, CRO at the Joint Research Centre (3000 scientists)
 - Founder and Head of CERT-EU 2011-2017
- Consultancy
 - Trusted Strategic Advisor
 - Advisor/Board Member in cybersecurity startups



Context

- Internet of Everything
 - Increased dependency
 - Everything connected
- Vulnerability Expanding
 - Inherently fragile
 - Frequently misconfigured, often unpatchable
- Agile Adversaries
 - Determined
 - Industrialized
 - Stealthy



Agenda

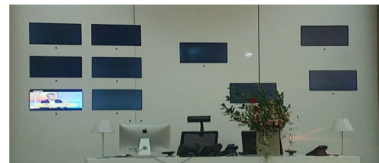
- Threats
- Prepare
- Adapt
- Contribute

Threats

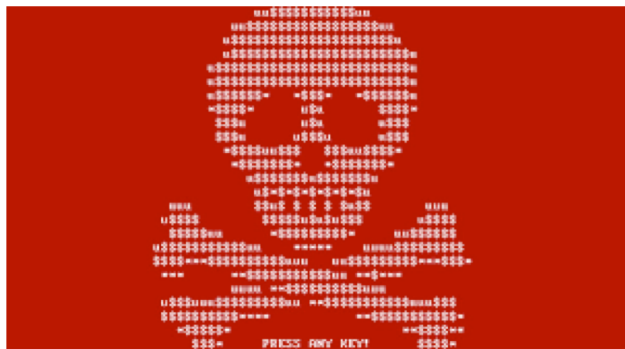
- Proliferation of Adversaries
- More Impact
- Proliferation of Techniques

Adversaries: Proliferation

- State-sponsored actors: more of the same and some more
 - Established players not afraid of being called out
 - New kids on the block copycatting established players
- Criminal groups
 - Streamlining operations
 - Specialization
 - Copycatting state-sponsored actors
- More dramatic (potential) impact

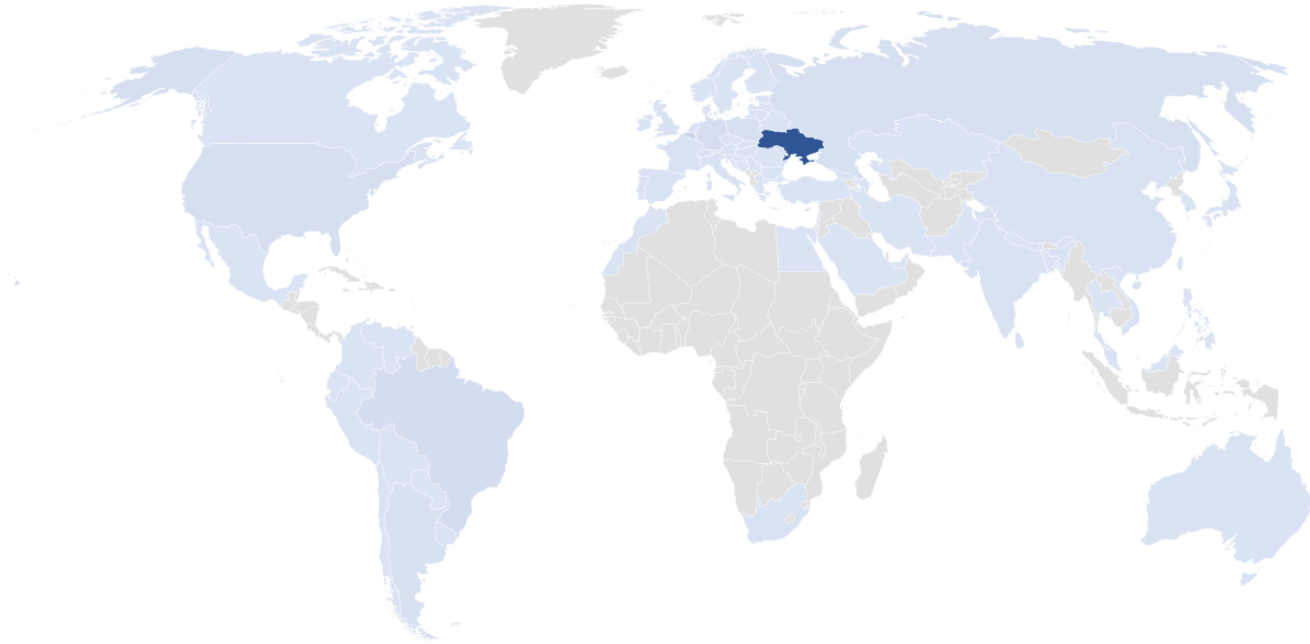


(Not)Petya



- Initial infection using legitimate software
- Spreading using a leaked NSA tool
- Destructive intent: no way to decrypt
- “Targeted”
- Massive collateral damage

Geographic distribution of Petya encounters



10% of all computers in UA destroyed
3 billion € collateral damage

Maersk/APM



- 17 container terminals disrupted for weeks
 - Loading and unloading impossible
 - Truck chaos
 - Reinstallation of 40.000 computers
 - Saved by power cut in Ghana...
-
- More than 300mio€ financial impact

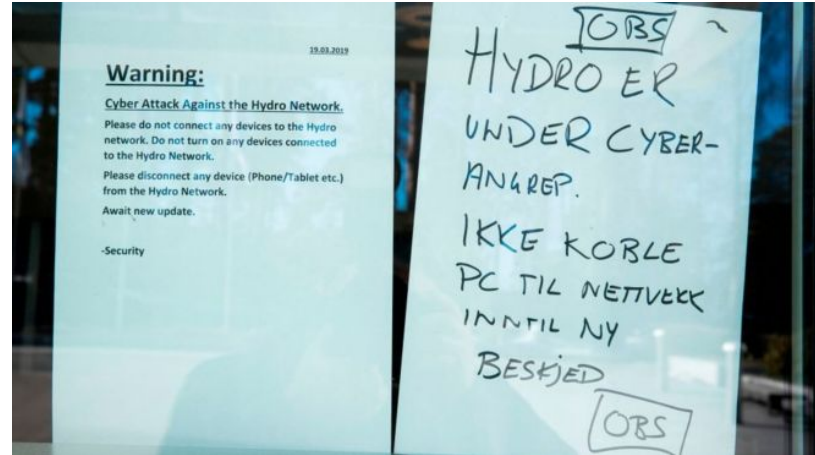
Big Game Hunting

Asco closure after cyber-attack to last another week

Saturday, 22 June 2019



© Belga



Eurofins Scientific: Forensic services firm paid ransom after cyber-attack

By Danny Shaw
Home affairs correspondent

🕒 5 July 2019

f 💬 🐦 ✉️ ➦ Share

Intermediate Questions

- Has your company been facing this type of problem?
- Does your company have a cyber insurance in place?
- Would your company pay ransom?
- Is this a Board issue in your company?
- How confident are you in your organisation's backup?

```
[~]$ shred
```


Techniques: Proliferation

- Leaked superweapons
- Blending in
- Broader surface

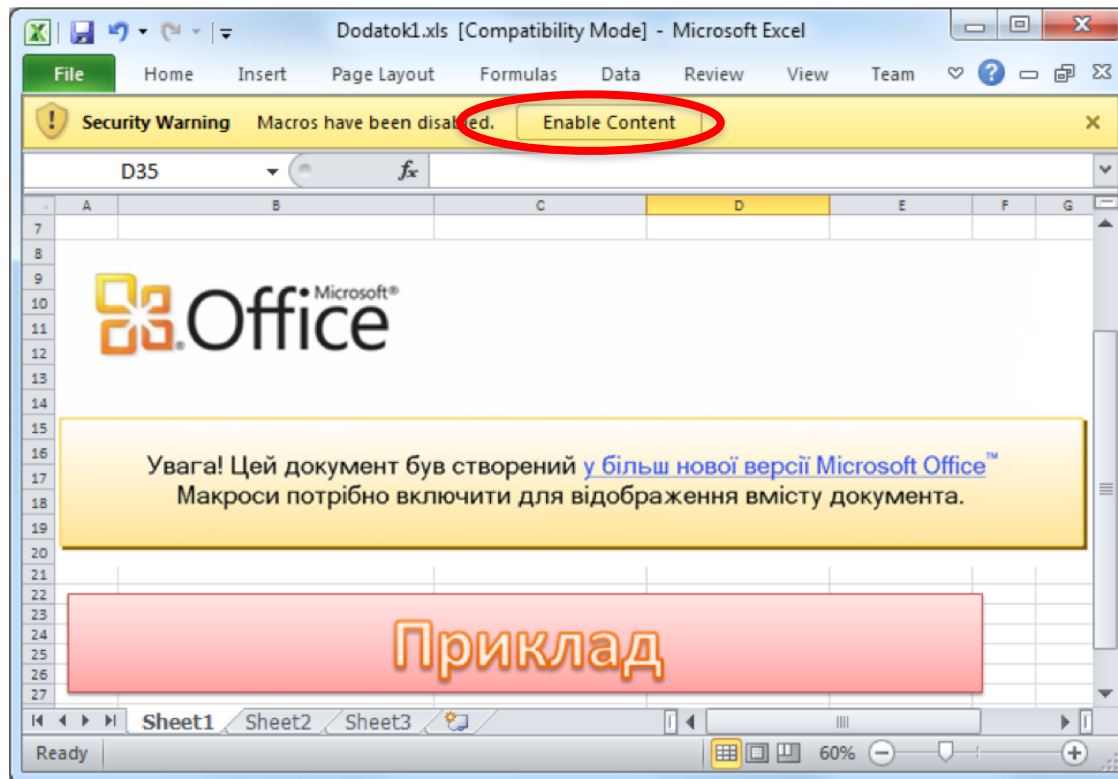
Leakage of Superweapons

- Espionage & law enforcement tools
 - Three letter agencies
 - Hacking Team
 - NSO
- Penetration and vulnerability testing tools
 - Mimikatz
 - Cobalt Strike
 - Metasploit
 - Bloodhound

Blending In

- Mails appearing as originating from a trusted origin
 - Typo squatting
 - Spoofed
 - Compromised
- Credible content
- Stealthy infection and lateral movements
 - Using legitimate credentials, replicating legitimate behavior
 - Abusing legitimate C&C infrastructure
 - Using legitimate tools (PowerShell, WMI, RDP)
 - Living off the land / file-less

Powershell



Targeting Us!

The image shows a Microsoft Word document interface. The ribbon at the top includes FILE, HOME, INSERT, DESIGN, PAGE LAYOUT, REFERENCES, MAILINGS, REVIEW, and VIEW. A yellow security warning bar is visible, stating "SECURITY WARNING: Macros have been disabled." with an "Enable Content" button circled in red. The document content includes the NCCIC (National Cyber Center of Interest) and FBI (Federal Bureau of Investigation) logos, a "JOINT ANALYSIS REPORT" header, a disclaimer, a reference number "JAR-16-20296A", and the title "Russian Malicious Cyber Activity".

FILE HOME INSERT DESIGN PAGE LAYOUT REFERENCES MAILINGS REVIEW VIEW Sign in

Read Mode Print Layout Web Layout Views

Outline Draft

Ruler Gridlines Navigation Pane Show

Zoom 100% One Page Multiple Pages Page Width

New Window Arrange All Split

View Side by Side Synchronous Scrolling Reset Window Position Window

Switch Windows Macros

SECURITY WARNING: Macros have been disabled. Enable Content

TLP:WHITE

DEPARTMENT OF HOMELAND SECURITY NCCIC

FEDERAL BUREAU OF INVESTIGATION Federal Bureau of Investigation

JOINT ANALYSIS REPORT

DISCLAIMER: This report is provided "as is" for informational purposes only. The Department of Homeland Security (DHS) does not provide any warranties of any kind regarding any information contained within. DHS does not endorse any commercial product or service referenced in this advisory or otherwise. This document is distributed as TLP:WHITE. Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction. For more information on the Traffic Light Protocol, see <https://www.us-cert.gov/tlp>.

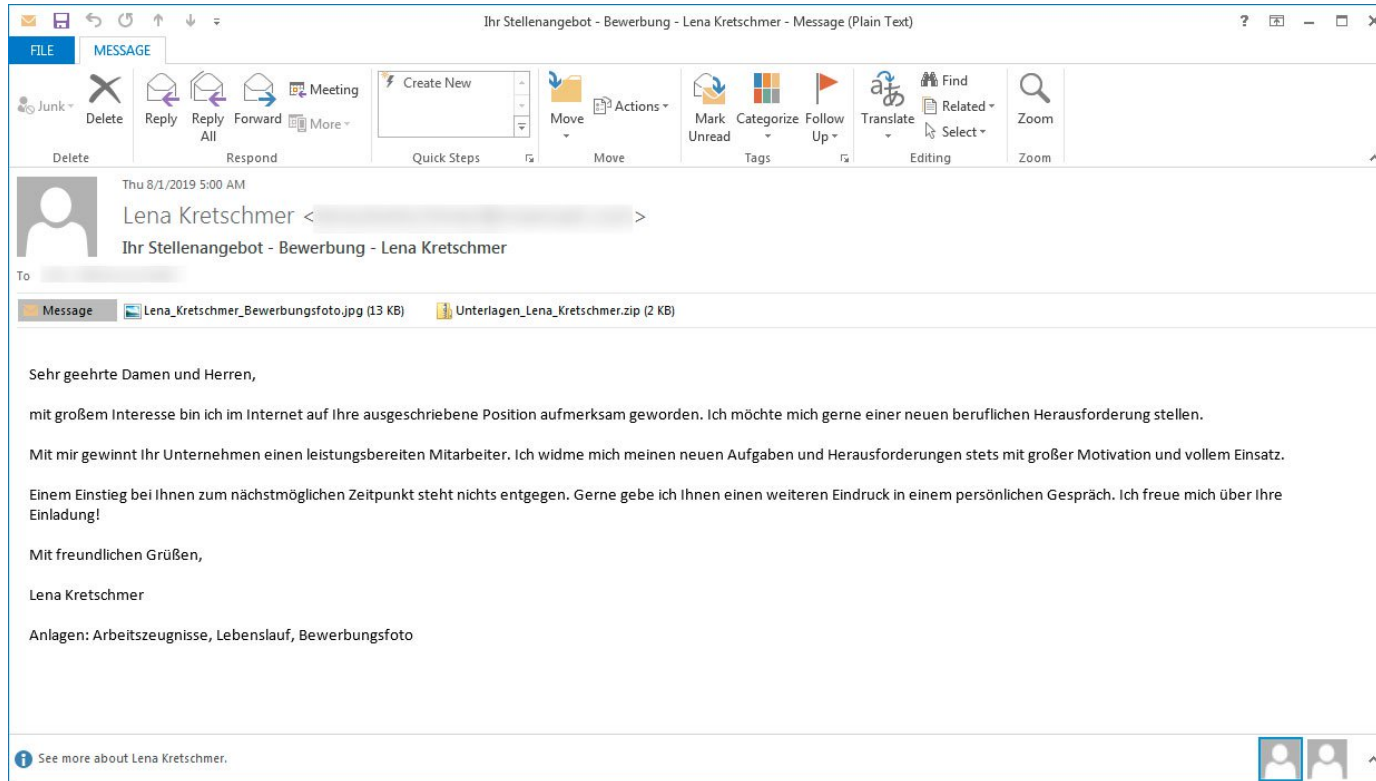
Reference Number: JAR-16-20296A December 29, 2016 **GRIZZLY STEPPE**

Russian Malicious Cyber Activity

Summary

This Joint Analysis Report (JAR) is the result of analytic efforts between the Department of Homeland Security (DHS) and the Federal Bureau of Investigation (FBI). This document provides technical details regarding the tools and infrastructure used by the Russian civilian and military intelligence Services (RIS) to compromise and exploit networks and endpoints associated with the U.S. election, as well as a range of U.S. Government, political, and private sector entities. The U.S. Government is referring to this malicious cyber activity by RIS as **GRIZZLY STEPPE**.

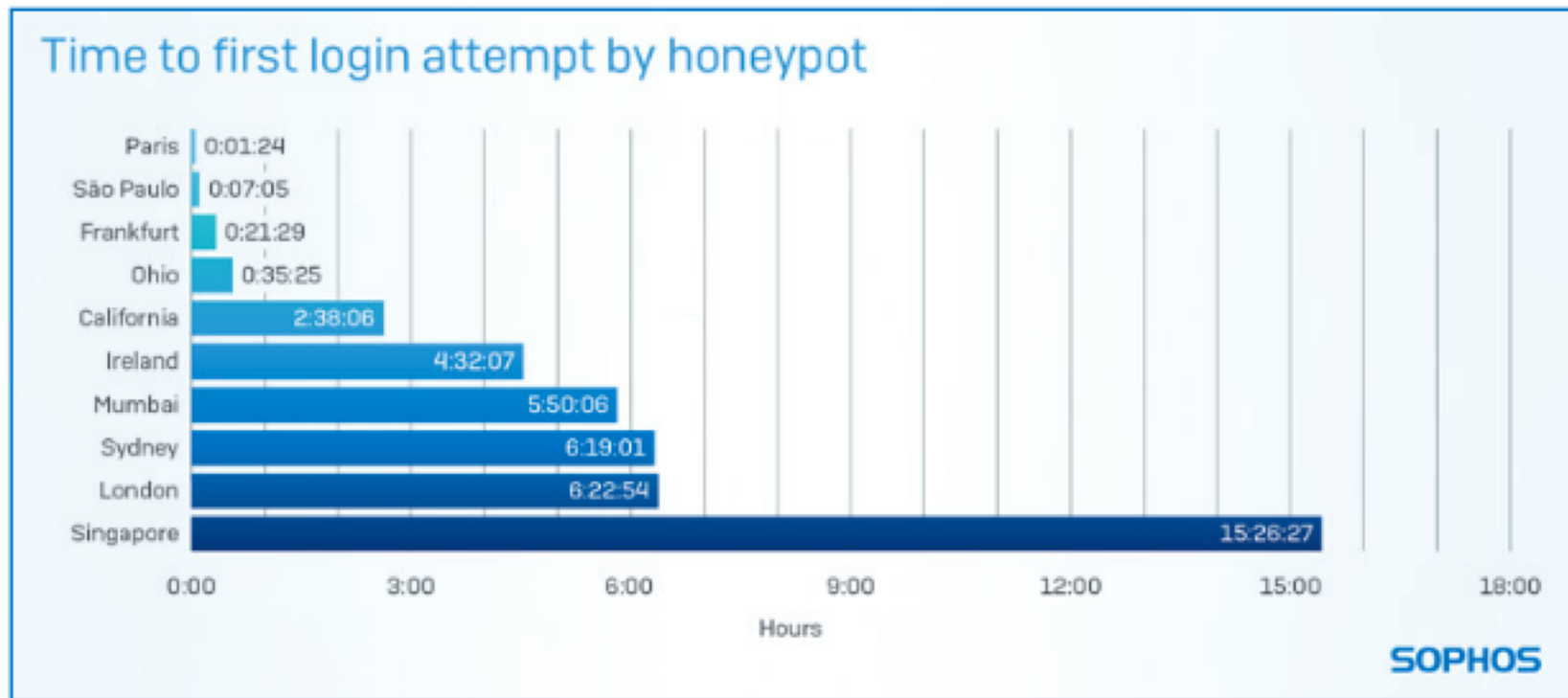
Credible



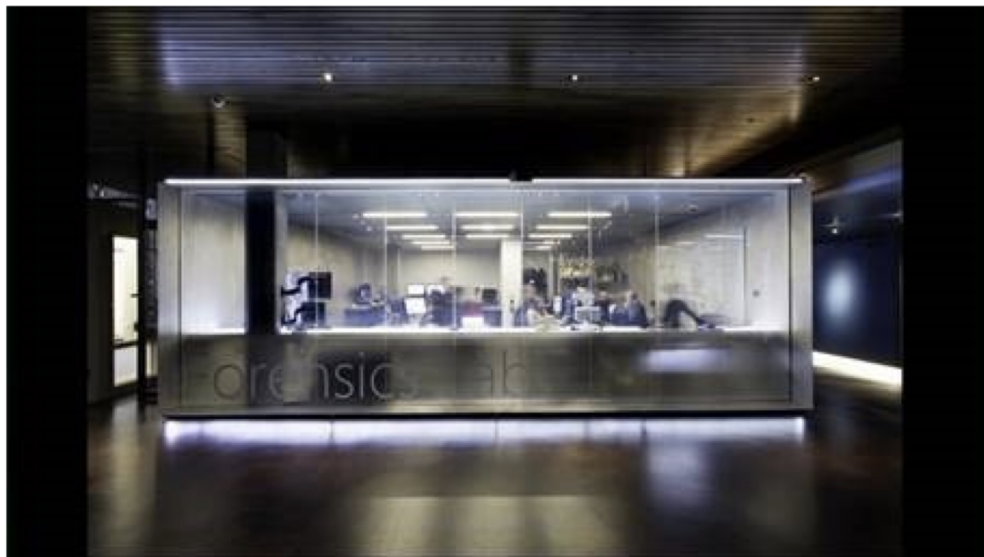
Broader Surface

- CMS/wiki/webrowsers
- Cloud, VMs
- Routers, switches
- Control systems, IOT
- Processors, firmware
- Credentials

Your RDP Open?



Your IOT Open?



Corporate IoT – a path to intrusion

Security Research & Defense / By MSRC Team / August 5, 2019 / Black Hat, IoT, MSTIC, STRONTIUM, Supply chain, Threat intelligence

Your Network Open?

Cisco Blogs



Cisco Blog > Security



Security

New Forensic Investigation Procedures for First Responder Guides



Lou Ronnau

August 30, 2019 - 1 Comment

Your Credentials Open?

```
C:\Users\John\Desktop>laZagne.exe browsers
```

```
=====
```

```
                        The LaZagne Project
```

```
                        ! BANG BANG !
```

```
=====
```

```
----- Internet Explorer passwords -----
```

```
Password found !!!
```

```
Username: zapata@yahoo.com
```

```
Password: Zapata_Uive!
```

```
Site: https://www.facebook.com/
```

```
----- Firefox passwords -----
```

```
Password found !!!
```

```
Website: https://accounts.google.com
```

```
Username: zapata@gmail.com
```

```
Password: LaLuchaSigue!
```

```
Password found !!!
```

```
Website: https://www.facebook.com
```

```
Username: che.guevara@gmail.com
```

```
Password: hasta_siempre!
```

```
[+] 3 passwords have been found.
```

```
For more information launch it again with the -v option
```

```
elapsed time = 0.120000123978
```

Agenda

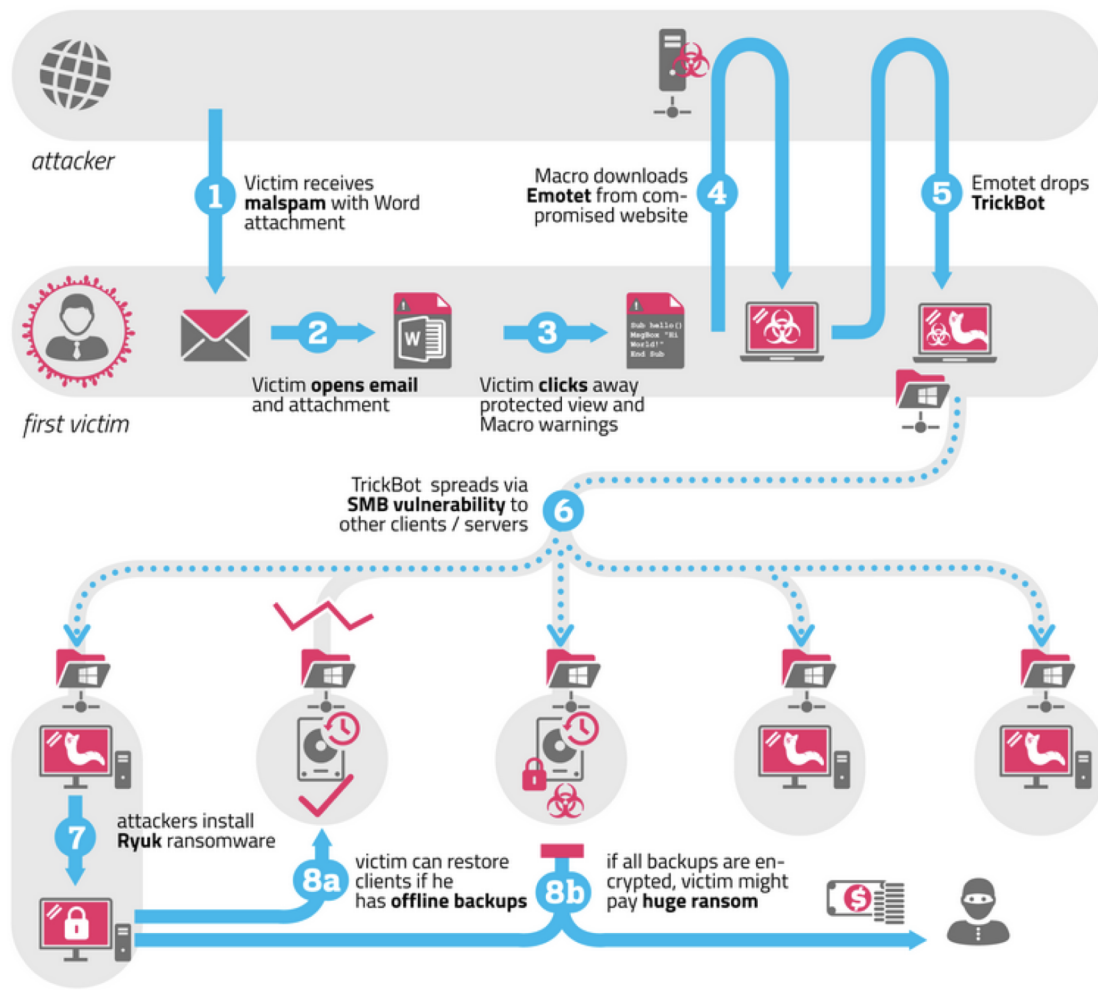
- Threats
- ***Prepare***
- Adapt
- Contribute

Prepare

- Prevent, detect, respond is not enough
- Gain visibility → ZEEK 😊
- Offline backups of your crown jewels
 - AD, configs, gold images, clients, orders...
- Manual fall backs / resilience
- Incident response plan - BCP
- Insurance / Legal support

Typical APT

- Find a weak entry point
- Scan the internal infrastructure
- Escalate privileges
- Move laterally
- Obtain keys to the Kingdom(s)
- Establish persistence (golden ticket, routers, bios, legit credentials)
- Detonate
- Return when you are kicked out



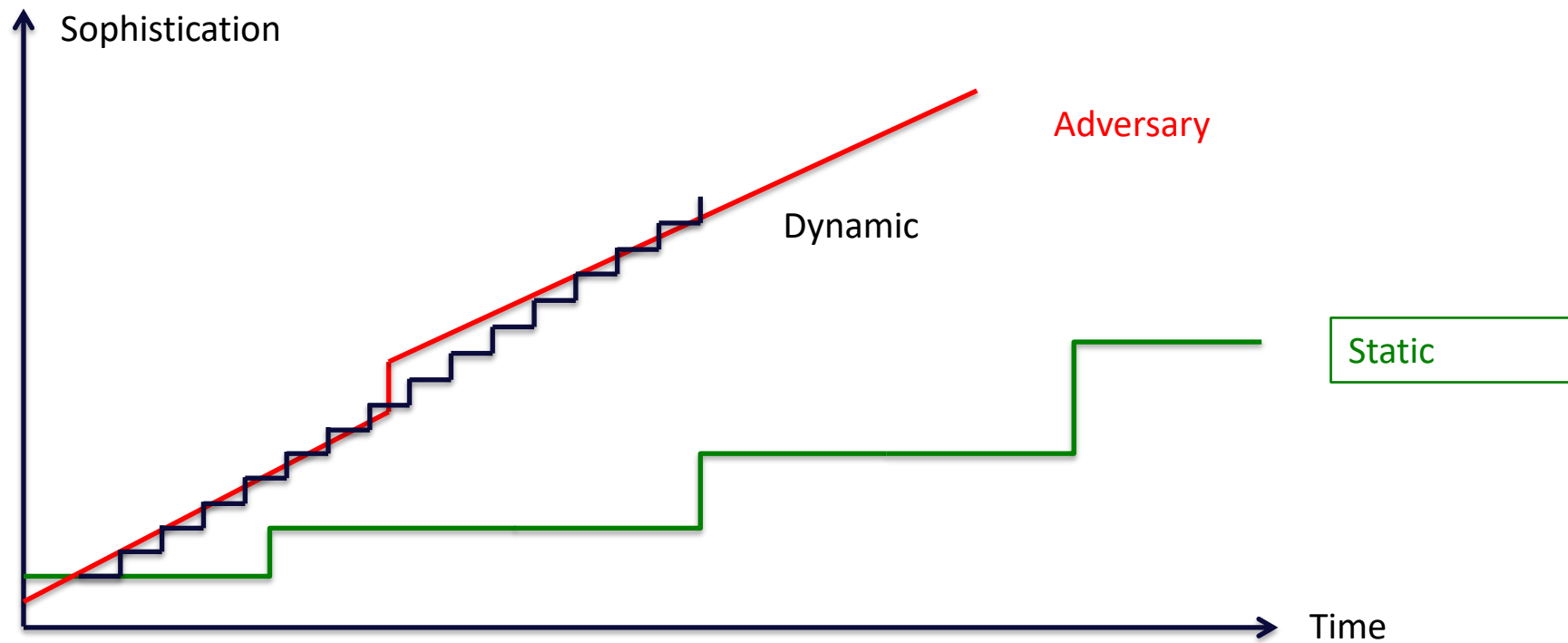
Agenda

- Threats
- Prepare
- ***Adapt***
- Contribute

Adapt

- Prevent, detect, respond are not static
- APT, the new normal
- Don't contain too quickly, **assume lateral movement**
- Internal reconnaissance can be noisy -> ZEEK 😊
- Move from Respond into Detect
- Track your adversaries and adapt your approaches

Gap

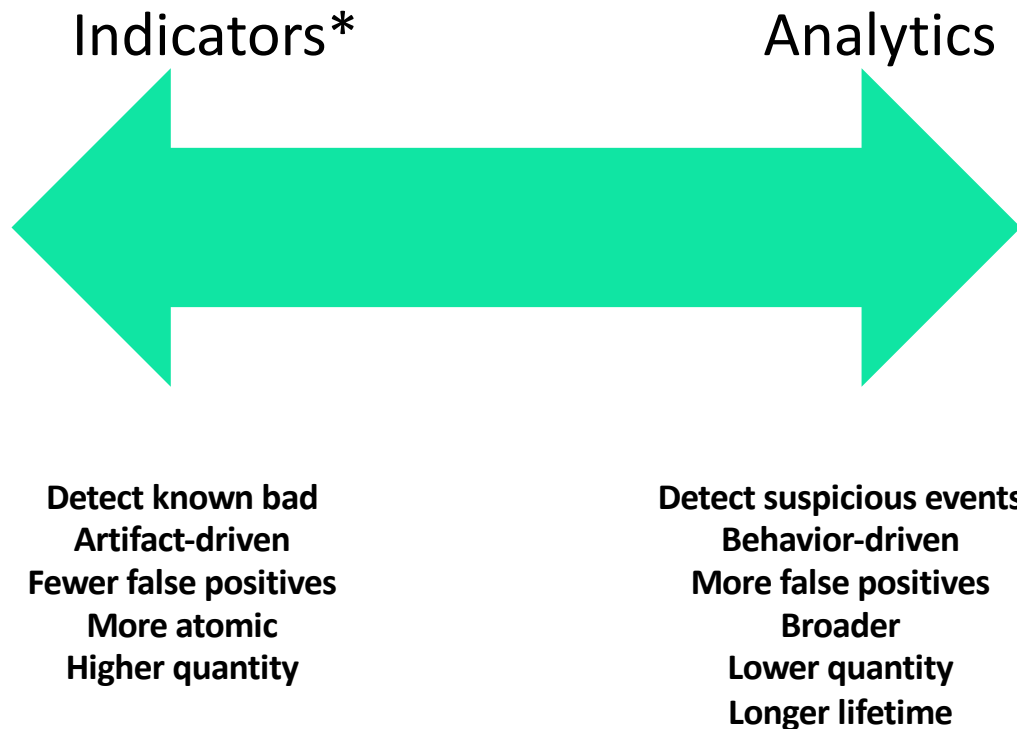


Gaps In Prevention/Detection

Lazarus x Fin7 x CIS 4 x Logs x Not detected by logs x +

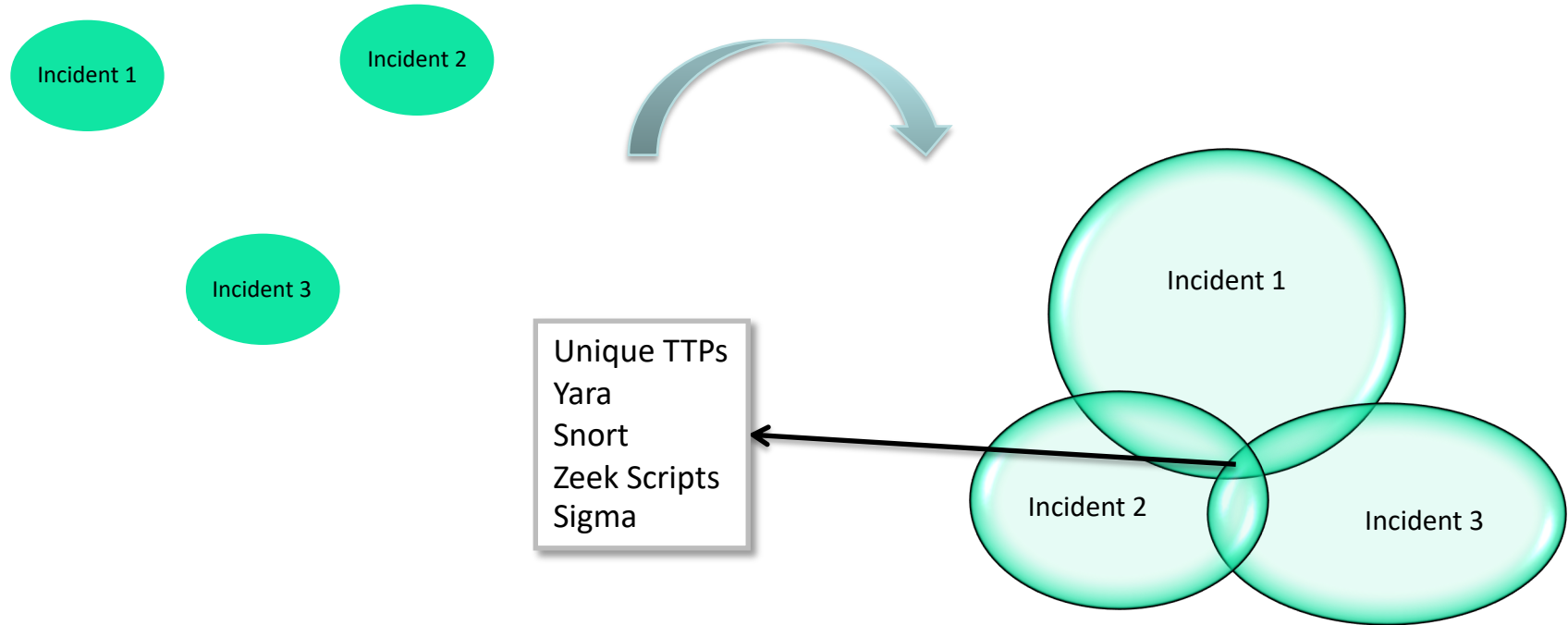
<div> <div>selection controls</div> <div>layer controls</div> <div>technique controls</div> </div>											
Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command And Control	Exfiltration	Impact
11 Items	33 Items	59 Items	28 Items	67 Items	19 Items	22 Items	17 Items	13 Items	22 Items	9 Items	14 Items
Drive-by Compromise	AppleScript	.bash_profile and .bashrc	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Account Discovery	AppleScript	Audio Capture	Commonly Used Port	Automated Exfiltration	Data Destruction
Exploit Public-Facing Application	CMSTP	Accessibility Features	Accessibility Features	Binary Padding	Bash History	Application Window Discovery	Application Deployment	Automated Collection	Communication Through Removable Media	Data Compressed	Data Encrypted for Impact
External Remote Services	Command-Line Interface	Account Manipulation	AppCert DLLs	BITS Jobs	Brute Force	Browser Bookmark Discovery	Software	Clipboard Data	Data Encrypted	Defacement	
Hardware Additions	Compiled HTML File	AppCert DLLs	AppInit DLLs	Bypass User Account Control	Credential Dumping	Domain Trust Discovery	Distributed Component Object Model	Data from Information Repositories	Connection Proxy	Data Transfer Size Limits	Disk Content Wipe
Replication Through Removable Media	Control Panel Items	AppInit DLLs	Application Shimming	Clear Command History	Credentials in Files	File and Directory Discovery	Exploitation of Remote Services	Data from Local System	Custom Command and Control Protocol	Exfiltration Over Alternative Protocol	Disk Structure Wipe
Spearphishing Attachment	Dynamic Data Exchange	Application Shimming	Bypass User Account Control	CMSTP	Credentials in Registry	Network Service Scanning	Logon Scripts	Data from Network Shared Drive	Custom Cryptographic Protocol	Exfiltration Over Command and Control Channel	Endpoint Denial of Service
Spearphishing Link	Execution through API	Authentication Package	DLL Search Order Hijacking	Code Signing	Exploitation for Credential Access	Network Share Discovery	Pass the Hash	Data from Removable Media	Data Encoding	Exfiltration Over Other Network Medium	Firmware Corruption
Spearphishing via Service	Execution through Module Load	BITS Jobs	Dylib Hijacking	Compile After Delivery	Forced Authentication	Network Sniffing	Pass the Ticket	Data Staged	Data Obfuscation	Exfiltration Over Physical Medium	Inhibit System Recovery
Supply Chain Compromise	Exploitation for Client Execution	Bootkit	Exploitation for Privilege Escalation	Compiled HTML File	Hooking	Password Policy Discovery	Remote Desktop Protocol	Email Collection	Domain Fronting	Exfiltration Over Physical Medium	Network Denial of Service
Trusted Relationship	Graphical User Interface	Browser Extensions	Component Firmware	Component Object Model Hijacking	Input Capture	Peripheral Device Discovery	Remote File Copy	Input Capture	Domain Generation Algorithms	Scheduled Transfer	Resource Hijacking
Valid Accounts	InstallUtil	Change Default File Association	Extra Window Memory Injection	Control Panel Items	Input Prompt	Permission Groups Discovery	Remote Services	Man in the Browser	Fallback Channels	Service Stop	Runtime Data Manipulation
	Launchctl	Component Firmware	File System Permissions Weakness	DCShadow	Kerberoasting	Process Discovery	Replication Through Removable Media	Screen Capture	Multi-hop Proxy	Stored Data Manipulation	
	Local Job Scheduling	Component Object Model Hijacking	Hooking	Deobfuscate/Decode Files or Information	Keychain	Query Registry	Shared Webroot	Video Capture	Multi-Stage Channels	Transmitted Data Manipulation	
	LSASS Driver	Create Account	Image File Execution Options Injection	Disabling Security Tools	LLMNR/NBT-NS Poisoning and Relay	Remote System Discovery	SSH Hijacking		Multiband Communication		
	Msihta	DLL Search Order Hijacking	Launch Daemon	DLL Search Order Hijacking	Network Sniffing	Security Software Discovery	Taint Shared Content		Port Knocking		
	PowerShell	Dylib Hijacking	New Service	DLL Side-Loading	Password Filter DLL	System Information Discovery	Third-party Software		Remote Access Tools		
	Regsvcs/Regasm	External Remote Services	Path Interception	Execution Guardrails	Private Keys	System Network Configuration Discovery	Windows Admin Shares		Remote File Copy		
	Regsvr32	File System Permissions Weakness	Plist Modification	Exploitation for Defense Evasion	Securityd Memory	System Owner/User Discovery	Windows Remote Management		Standard Application Layer Protocol		
	Rundll32	Hidden Files and Directories	Port Monitors	Extra Window Memory Injection	Two-Factor Authentication Interception	System Service Discovery			Standard Cryptographic Protocol		
	Scheduled Task	Hooking	Process Injection	File Deletion		System Time Discovery			Standard Non-Application Layer Protocol		
	Scripting	Hypervisor	Scheduled Task	File Permissions Modification		Virtualization/Sandbox Evasion			Uncommonly Used Port		
	Service Execution	Image File Execution Options Injection	Service Registry Permissions Weakness	File System Logical Offsets					Web Service		
	Signed Binary Proxy Execution	Signed Script Proxy Execution	Kernel Modules and Extensions	Gatekeeper Bypass							
	Source		Setuid and Setgid	Group Policy Modification							

Analytics Instead of Indicators

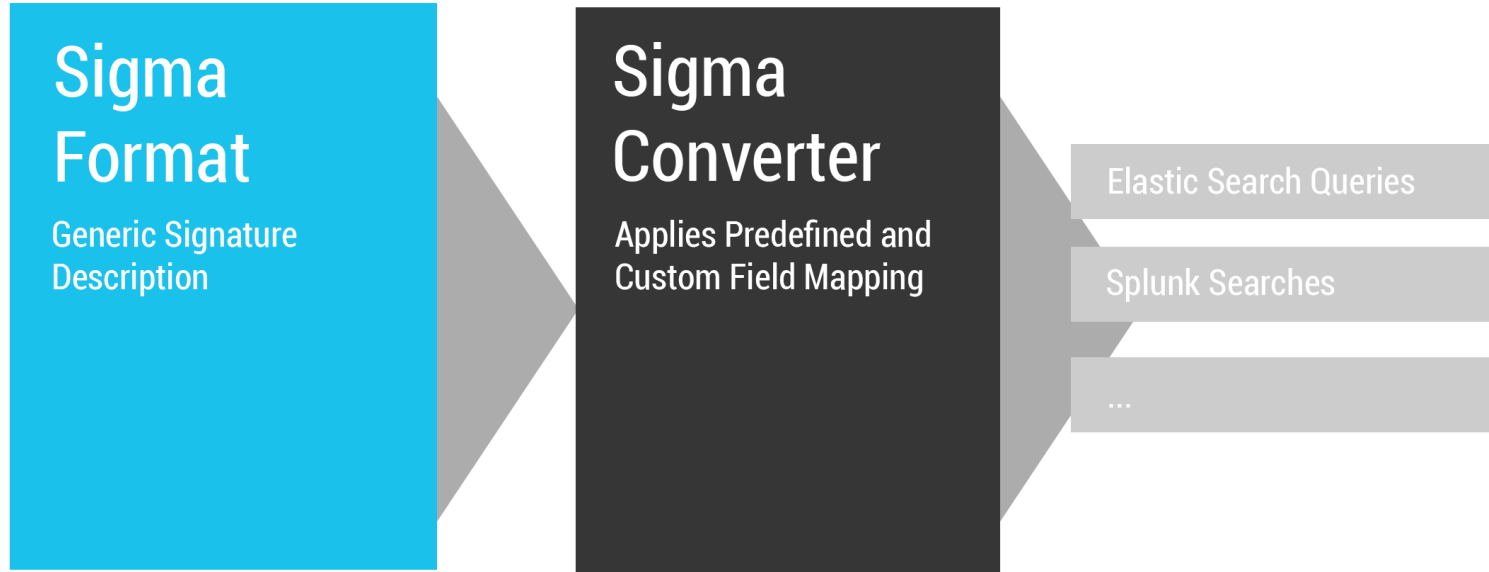


*good, fresh, indicators are useful too

TTPs are more stable



Analytics in SIGMA



<https://github.com/Neo23x0/sigma>

Sample SIGMA Rule

title: Renamed PowerShell

status: experimental

description: Detects the execution of a renamed PowerShell often used by attackers or malware

references:

- <https://twitter.com/christophetd/status/1164506034720952320>

author: Florian Roth

date: 2019/08/22

tags:

- car.2013-05-009

logsource:

product: windows

service: sysmon

detection:

selection:

Description: Windows PowerShell

Company: Microsoft Corporation

filter:

Image: '*\powershell.exe'


condition: selection and not filter


falsepositives:


- Unknown


level: critical


SIGMA Rules


 **Neo23x0** / **sigma**


 Watch 196


 Star 1,441


 Fork 345


 Code


 Issues 40

 Pull requests 14

 Projects 1


 Wiki

 Security









 Insights

Branch: master ▾ **sigma** / **rules** / **apt** /

Create new file Find file History

 **megan201296** Create apt_oceanlotus_registry.yml ... Latest commit 74fce5f on 14 Apr

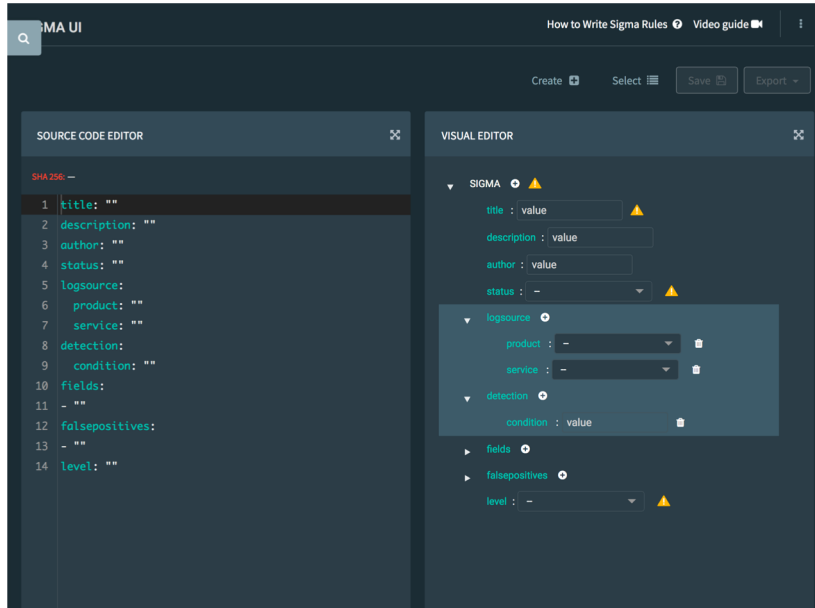
..

 apt_apt29_thinktanks.yml	add tags to apt29 thinktanks rule	3 months ago
 apt_apt29_tor.yml	fix tags on apt29 tor rule	3 months ago
 apt_babyshark.yml	add tags to apt babyshark rule	3 months ago
 apt_bear_activity_gtr19.yml	fix and add tags to apt bear activity gtr19 rule	3 months ago
 apt_carbonpaper_turla.yml	fix tags in apt carbonpaper turla rule	3 months ago
 apt_chafer_mar18.yml	Converted to use the new process_creation data source	3 months ago
 apt_cloudhopper.yml	updated to use process_creation	4 months ago
 apt_dragonfly.yml	updated to use process_creation	4 months ago

SIGMA Tools

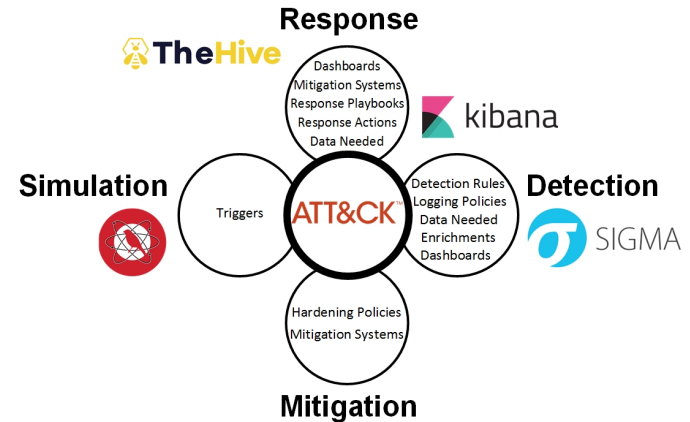
SIGMA Editor

<https://github.com/socprime/SigmaUI>





Atomic Threat Coverage


<https://github.com/krakow2600/atomic-threat-coverage>




Zeek Packages

 **293** commits

 **3** branches

 **0** releases


 **38** contributors











Branch: **master** ▾

New pull request

Find File

Clone or download ▾

 **Robin Sommer** Update aggregated metadata. Latest commit d301c01 4 hours ago

 Oxxon	Rename a few packages from Bro to Zeek	9 months ago
 activecm	Add Bro MongoDB logging writer package	2 years ago
 anthonykasza	add: anthonykasza index	9 months ago
 apache	Add metron-bro-plugin-kafka package	2 years ago
 bricata	Added bricata	last year
 bro	Added the official Bro NETMAP plugin	2 years ago
 corelight	Add the Corelight QUIC protocol analyzer/detector	last year
 cybera	Adding Cybera Sniffpass module	last month
 dopheide	Merge branch 'master' of https://github.com/dopheide/packages	2 months ago
 dovehawk	added dovehawk anonymized flow collector	17 days ago

Agenda

- Threats
- Prepare
- Adapt
- ***Contribute***

Contribute

- Prevent, detect, respond are can inspire others
- **Provide feedback and contribute analytics** to the Community
- Crowdsourced behavioral detection libraries
- Sharing TTPs/SIGMA/ZEEK rules is easier than sharing IOCs
- It's also more useful
 - More context
 - More stable in time
- **Defense: Proliferation**

EU ATT&CK User Community

- Mailing list -> opt in ? -> email to info@circl.lu
- User conference in Brussels 18-19 May 2020

Workshop - EU ATT&CK Community

Next workshop - event for EU ATT&CK Community

Conclusion

- The Threats Are Changing
- And So Are We:
 - Preparing
 - Adapting
 - Contributing



Thank You

Don't Hide The Risk, Manage It

www.FreddyDezeure.eu