digital shadows_

University of Thessaly

January 2019

Incident Response and CTI: Applied methodology and tools

Isidoros Monogioudis, Senior Security Engineer/Architect

Isidoros.monogioudis@digitalshadows.com
Isidoros.mon@gmail.com

digital shadows_

Threat landscape

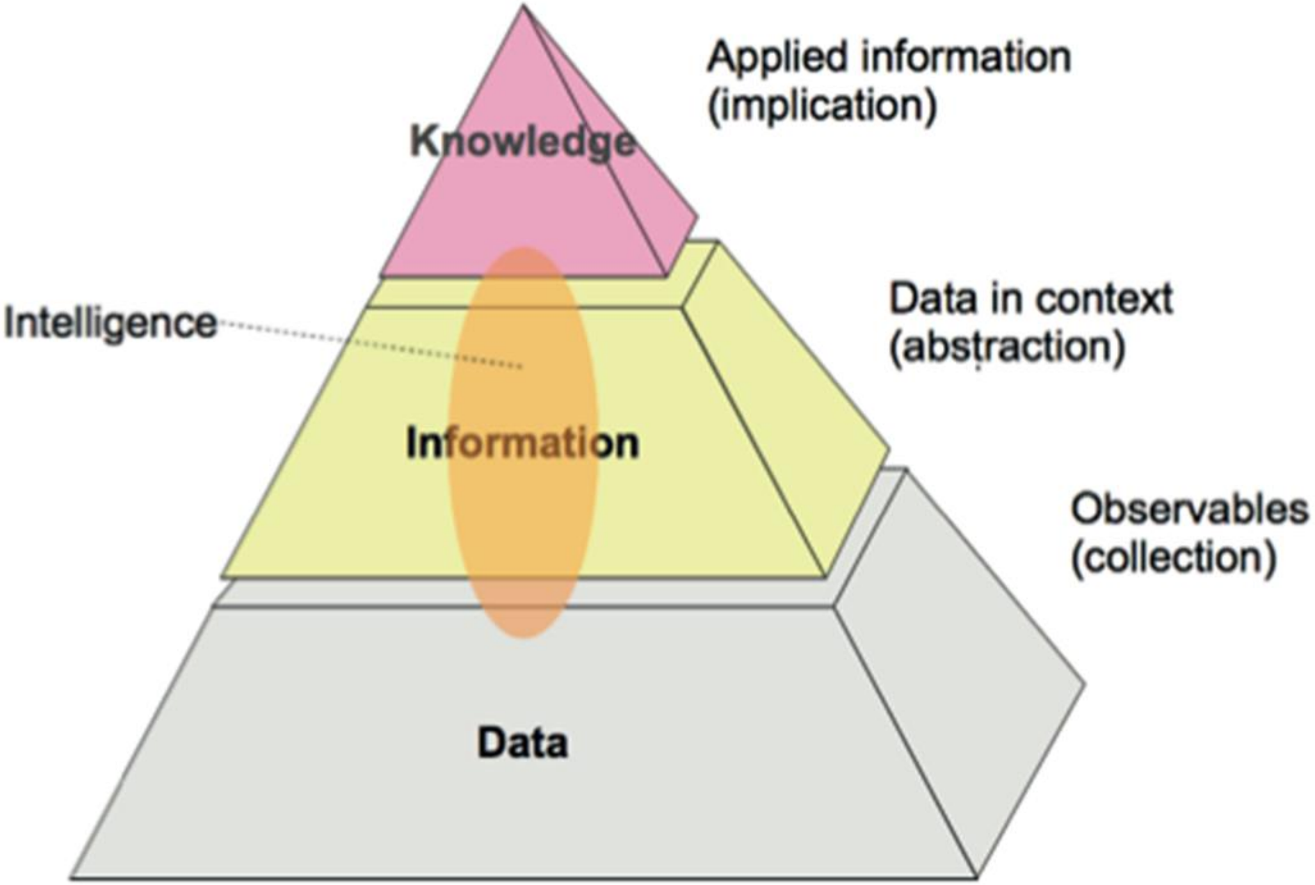
- Hacktivists
  - Anonymous
- Unintentional/intentional insiders
  - FedEx (S3 bucket)/Jiaqiang Xu/IBM
- Competent individual hackers
  - Phineas Fisher
- Organized Criminal Groups
  - FIN7, FIN4, Carbanak, Cobalt
- Nation state proxies
  - Syrian Electronic Army (SEA)
- Nation states
  - Foreign intelligence services (FSB or SVR) or militaries (PLA or GRU)

Cyber Threat Intelligence

- Definition of Threat
  - an expression of intent to do harm, i.e. deprive, weaken, damage or destroy;
  - an indication of imminent harm;
  - an agent that is regarded as harmful;
  - a harmful agent’s actions comprising of tactics, techniques, and procedures (TTPs).

Cyber Threat Intelligence

- Definition of Intelligence



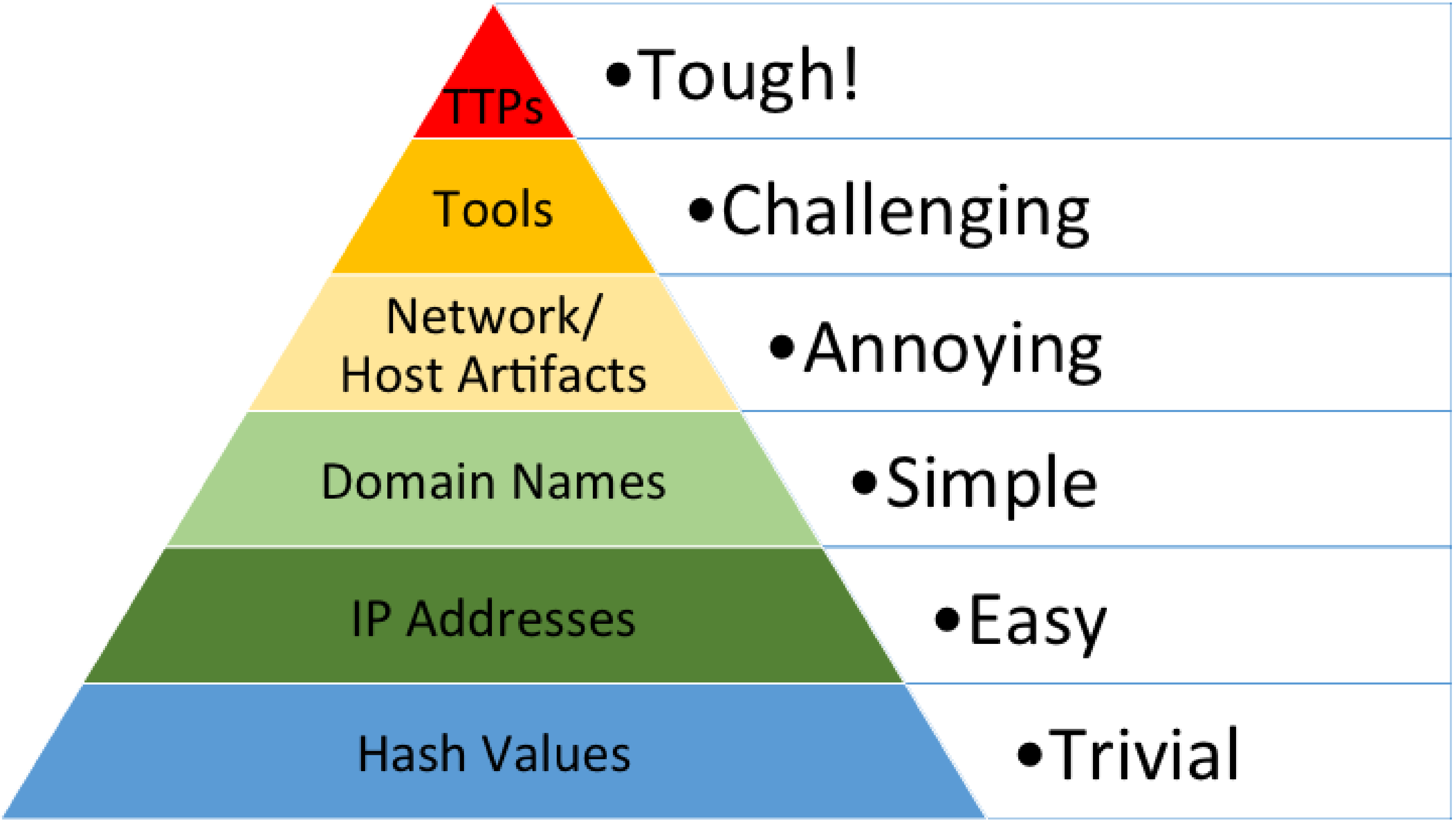
Cyber Threat Intelligence

- Information about threats and threat actors that provides sufficient **understanding to mitigate a harmful event** in the cyber domain
- The purpose of intelligence is:

“improving decision making by reducing ignorance”

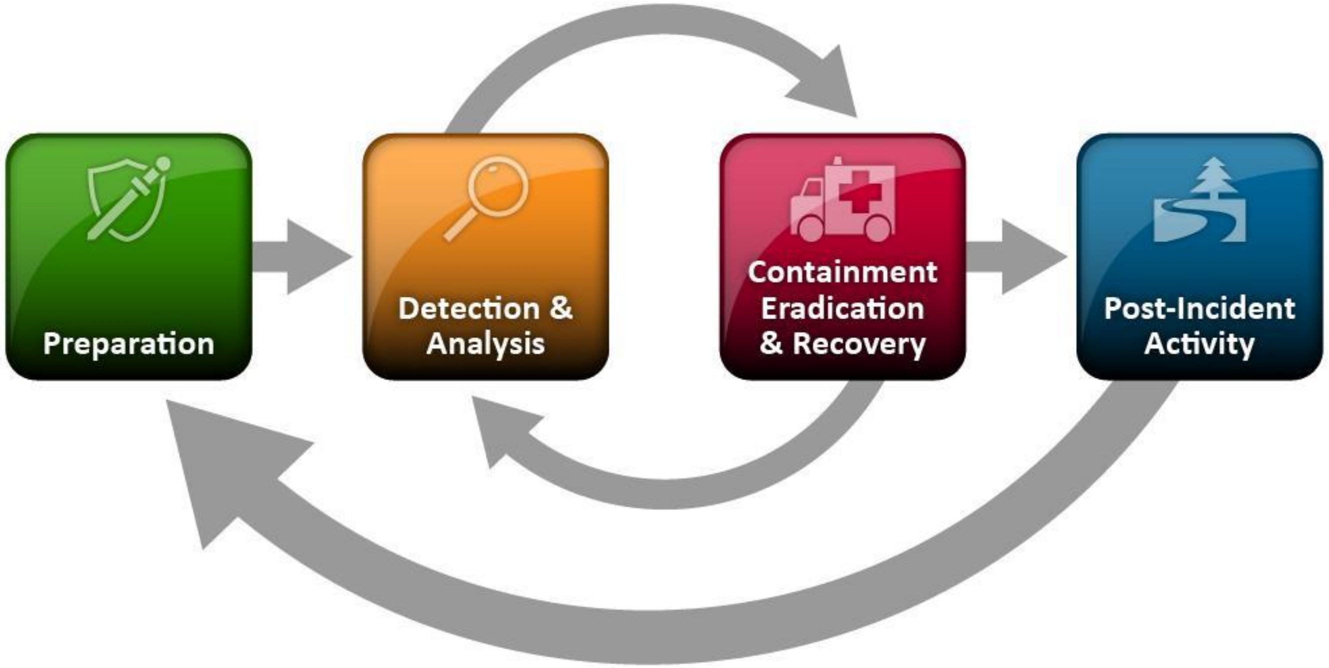
Sir David Omand, Former Director, GCHQ

Threat Intelligence "Pyramid of Pain"



TTPs	•Tough!
Tools	•Challenging
Network/ Host Artifacts	•Annoying
Domain Names	•Simple
IP Addresses	•Easy
Hash Values	•Trivial

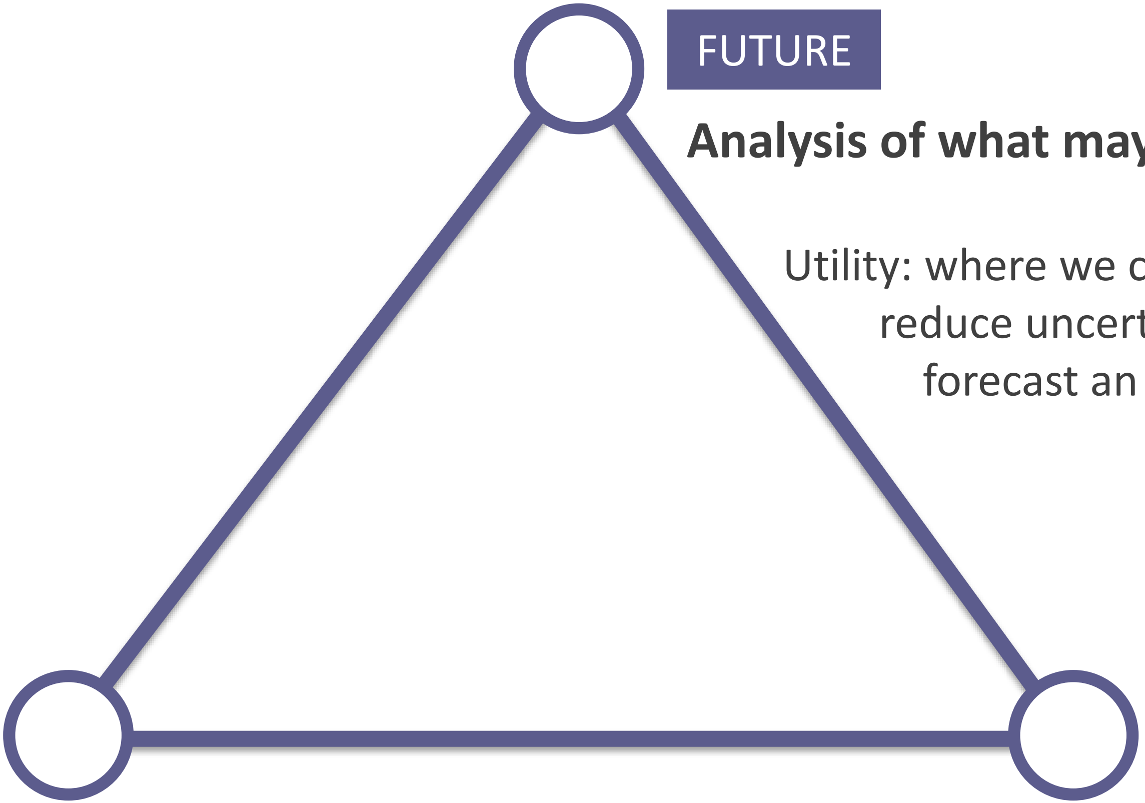
Incident Response Process



Preparation

Preparation	
Incident Response	**Threat Intelligence**
Building Malware analysis Skills	Building Threat analysis skills
Facilitating Communication and Coordination	-//-
Acquiring Tools and resources	-//-
Study Attack kill chain	Study attack kill chain

Intelligence Concerns



FUTURE

Analysis of what may happen.

Utility: where we can usefully reduce uncertainty to better forecast an outcome.

PAST

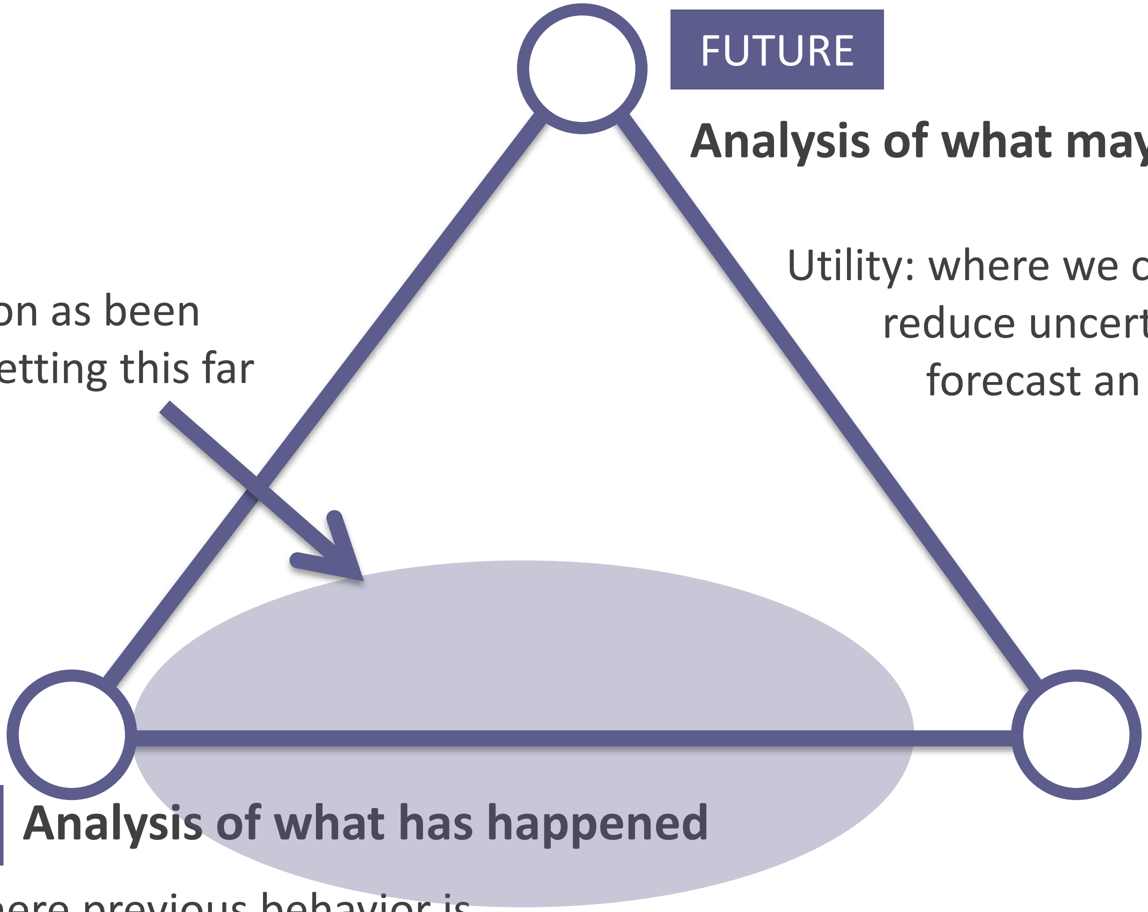
Analysis of what has happened

Utility: where previous behavior is an indicator of future behavior.

NOW

Utility: where we can respond more effectively with clarity in the knowledge of what is unfolding in front of us.

Intelligence Concerns



FUTURE

Analysis of what may happen.

Utility: where we can usefully reduce uncertainty to better forecast an outcome.

Our profession as been historically getting this far

PAST

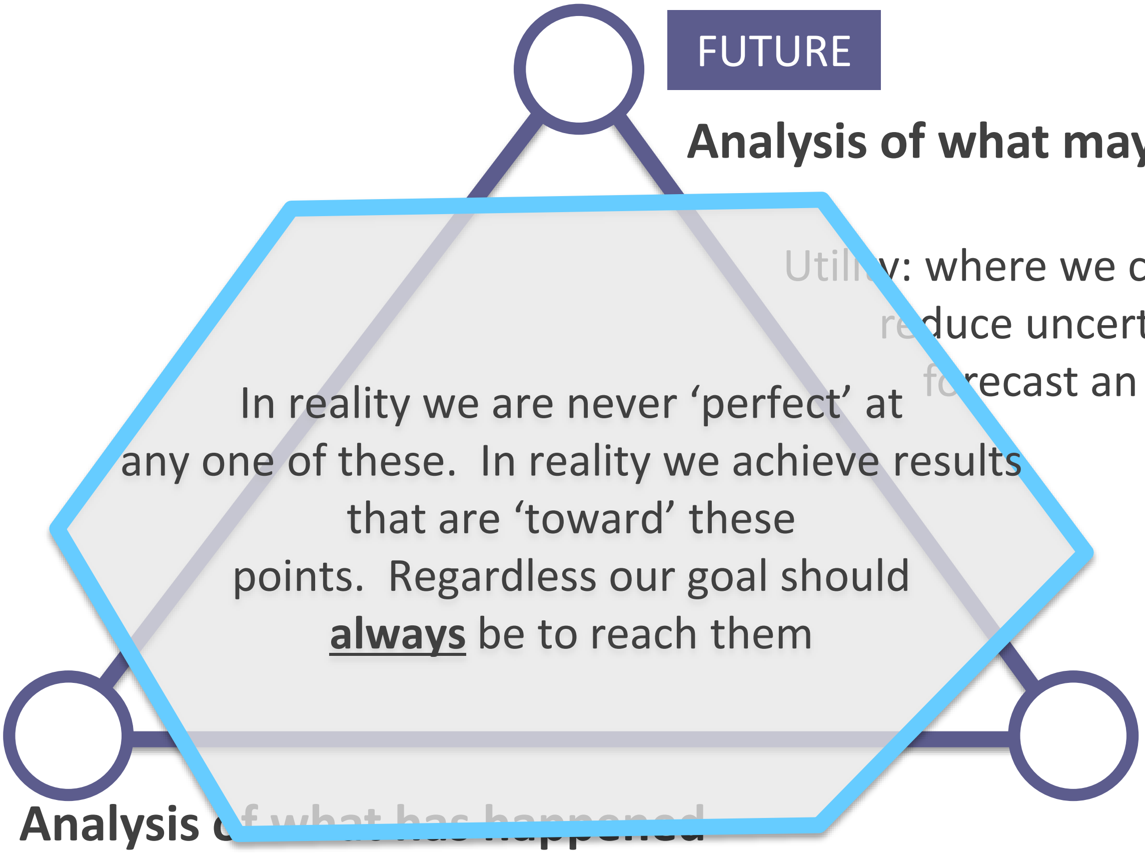
Analysis of what has happened

Utility: where previous behavior is an indicator of future behavior.

NOW

Utility: where we can respond more effectively with clarity in the knowledge of what is unfolding in front of us.

Intelligence Concerns



FUTURE

Analysis of what may happen.

Utility: where we can usefully reduce uncertainty to better forecast an outcome.

In reality we are never 'perfect' at any one of these. In reality we achieve results that are 'toward' these points. Regardless our goal should **always** be to reach them

NOW

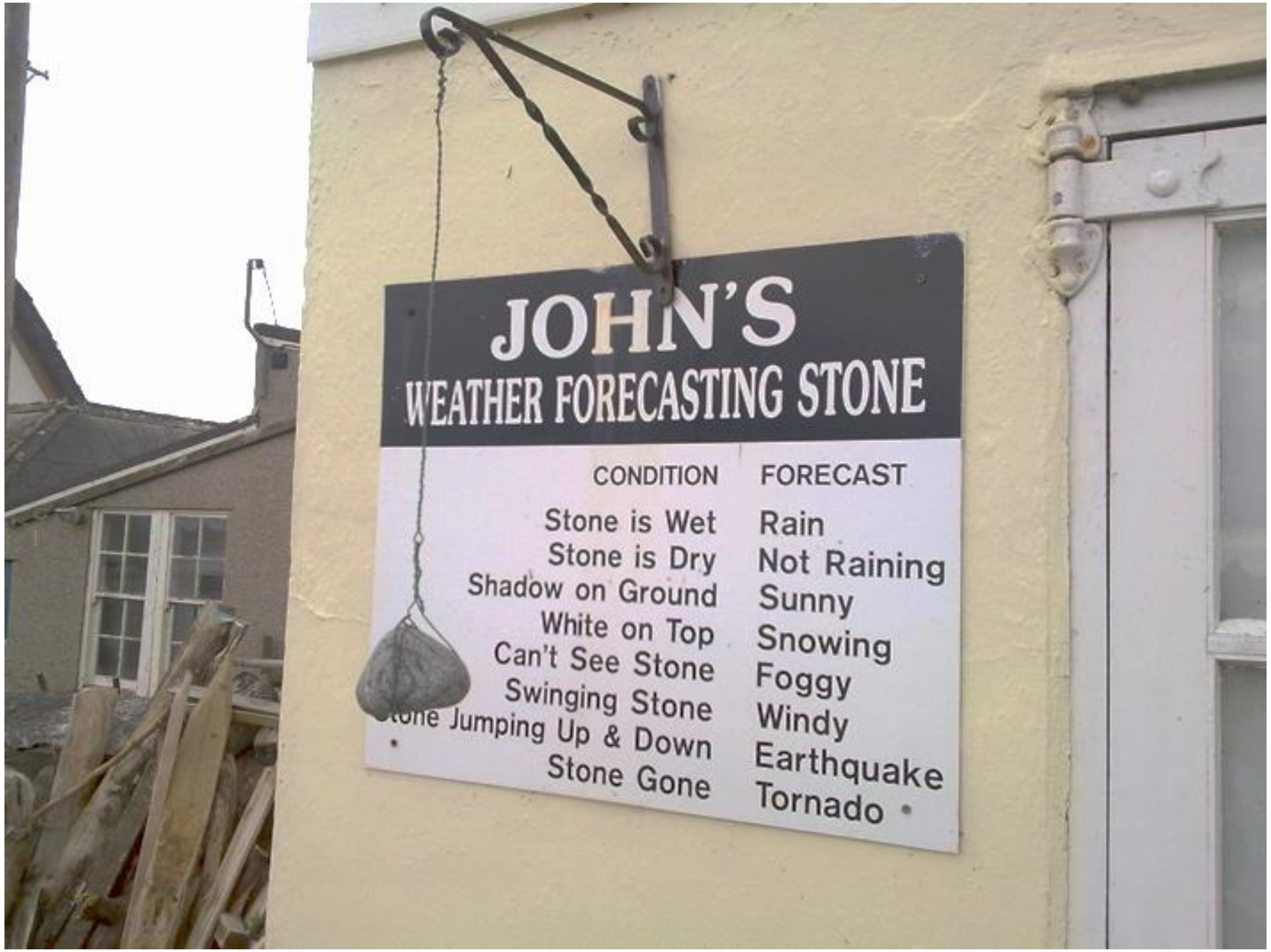
Utility: where we can respond more effectively with clarity in the knowledge of what is unfolding in front of us.

PAST

Analysis of what has happened

Utility: where previous behavior is an indicator of future behavior.

Forecasting



JOHN'S

WEATHER FORECASTING STONE

CONDITION	FORECAST
Stone is Wet	Rain
Stone is Dry	Not Raining
Shadow on Ground	Sunny
White on Top	Snowing
Can't See Stone	Foggy
Swinging Stone	Windy
tone Jumping Up & Down	Earthquake
Stone Gone	Tornado

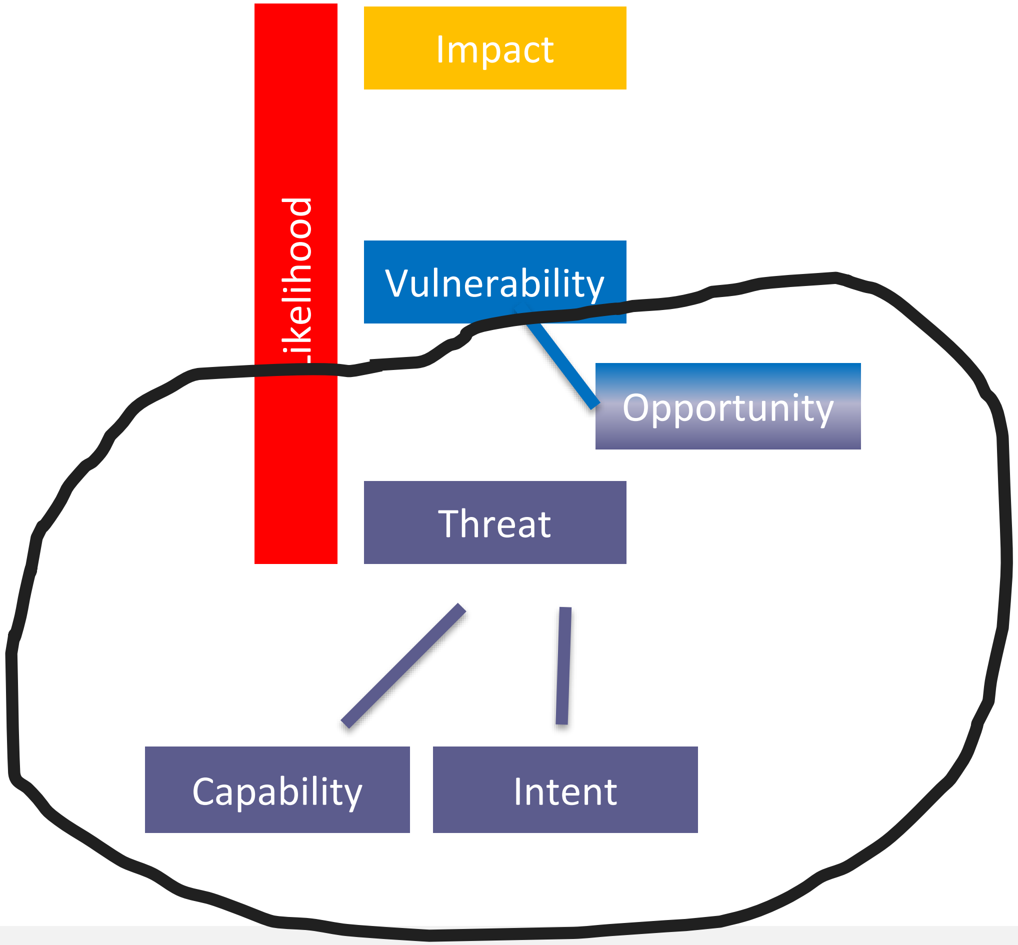
Forecasting

- **Warnings and Indicators:** Pre-cursor activities that might indicate future intent.

- **Human Intelligence (HUMINT):** information gathered from the planning activities of a campaign from those with the intent

- **Pattern extrapolation:** if see a sequence in attacks emerging, it is reasonable to assume an increase in threat for similar organizations

Better guesses

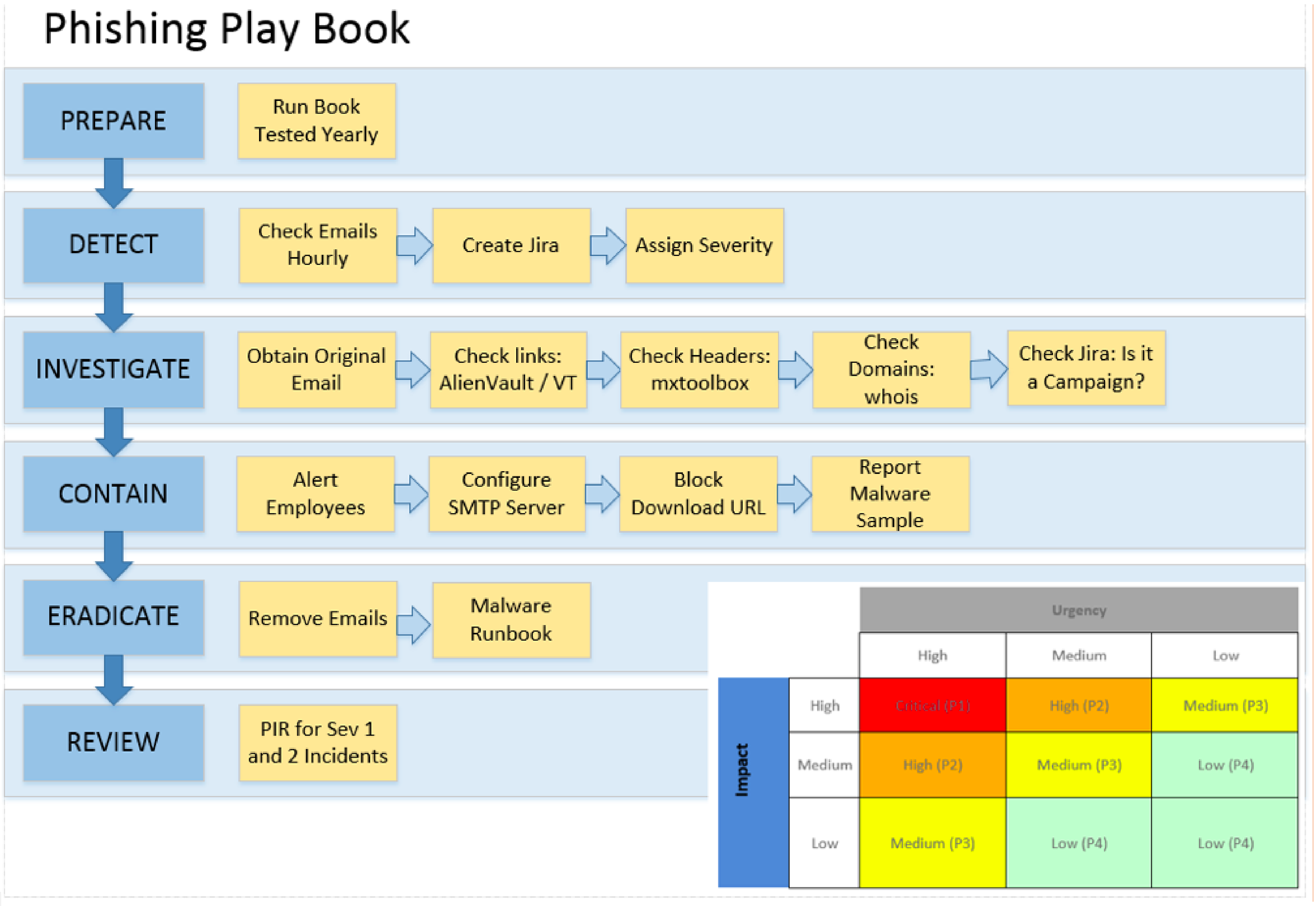


Know what info assets you hold where

Measure how an attacker views your business

Forecast current and future threat environment

Playbooks



Phishing Play Book

PREPARE: Run Book Tested Yearly

DETECT: Check Emails Hourly → Create Jira → Assign Severity

INVESTIGATE: Obtain Original Email → Check links: AlienVault / VT → Check Headers: mxtoolbox → Check Domains: whois → Check Jira: Is it a Campaign?

CONTAIN: Alert Employees → Configure SMTP Server → Block Download URL → Report Malware Sample

ERADICATE: Remove Emails → Malware Runbook

REVIEW: PIR for Sev 1 and 2 Incidents

		Urgency		
		High	Medium	Low
Impact	High	Critical (P1)	High (P2)	Medium (P3)
	Medium	High (P2)	Medium (P3)	Low (P4)
	Low	Medium (P3)	Low (P4)	Low (P4)

Detection and Analysis

Detection and Analysis	
Incident Response	**Threat Intelligence**
Identifying Malware Incident Characteristics	Identifying IOCs
Identifying Infected Hosts	Applying IOCs
Malware behaviour	Related malware study
Malware impact	Related malware evidence

Detection Methods

Network and Computer Artefacts

- Netflow
- Whitelisting
- Intrusion Detection Systems (IDS)
- Endpoint detection and response (EDR)
- Security Incident Event Monitoring (SIEM)

People and Process

- Awareness (People Spidey Sense)
- Process Controls
- Human Pattern Identification
- Hotline and reporting
- Customer Reporting Hotline (Support)

Indicators of Compromise

- Forensic artefacts observed on a network signifying an intrusion

Domains	Fast flux / DGA in malware
Hashes	Polymorphism
IP	Anonymization / VPN
Thread/Process	Detection tricky
Files / File Artefacts	In Memory
Registry	Repurposing existing tools (PowerShell)

Indicators of Compromise

- Forensic artefacts observed on a network signifying an intrusion

Domains

H

Threa

Files / F

Registry

Fast flux / DGA in malware

sm

/ VPN

icky

y

Repurposing existing tools (PowerShell)

Tactics Techniques and Procedures (TTPs)

- TTPs are the “patterns of activities or methods associated with a specific threat actor or group of threat actors”
- Tactics: **WHAT**
  - (Initial Access, Execution, Persistence, Privilege Escalation, Defense Evasion, Credential Access, Discovery, Lateral Movement, Collection, Exfiltration, Command and Control).
- Technique: **HOW**
  - **(Initial Access:** Drive-by Compromise, Exploit public-facing application, Spearphishing attachment, Supply chain compromise etc.)
- Procedure: **more HOW** (tools, scripts, commands)
  - Sqlmap, havij tools for “exploit public-facing applications” used to automate SQL injection

TTPs - Mitre PRE-ATT&CK

- “This cyber threat framework captures the tactics, techniques, and procedures adversaries use to select a target, obtain information, and launch a campaign.”

Priority Definition
- Planning, Direction

Target Selection

Information Gathering
- Technical, People, Organizational

Weakness Identification
- Technical, People, Organizational

Adversary OpSec

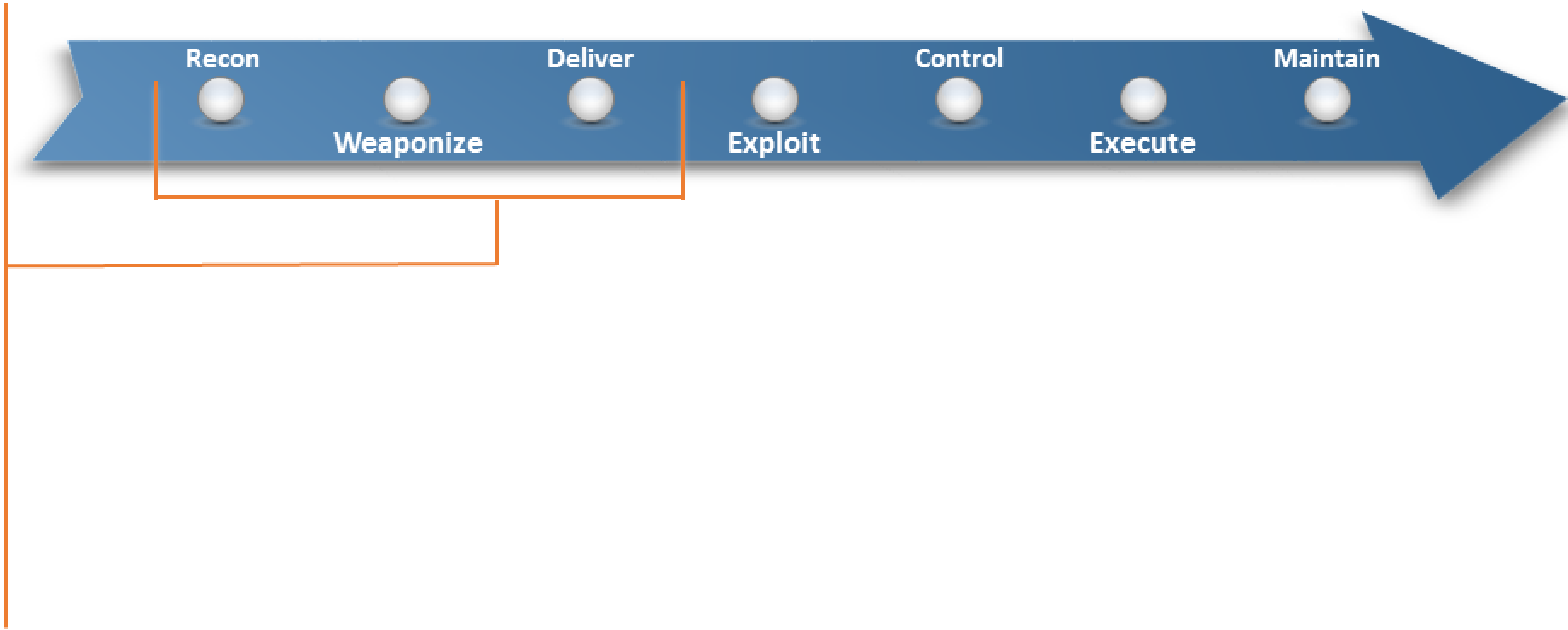
Establish & Maintain Infrastructure

Persona Development

Build Capabilities

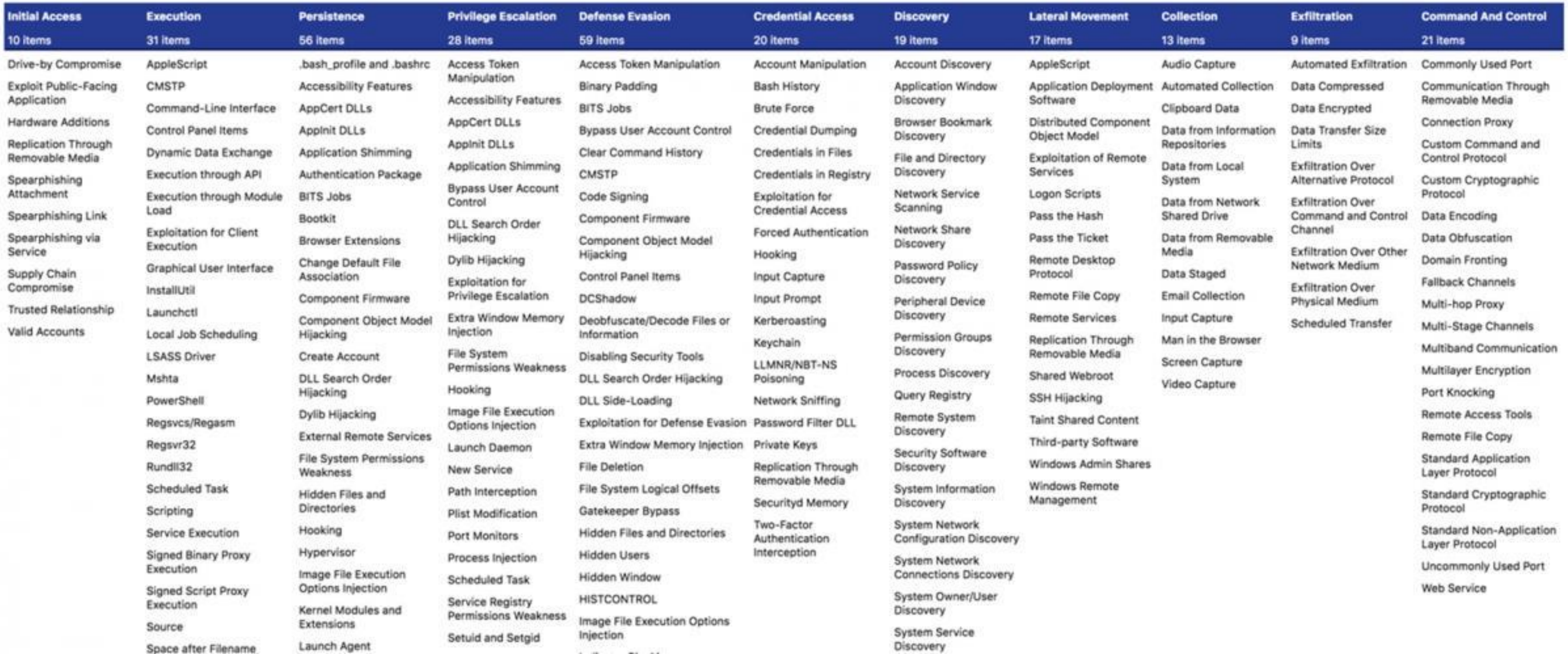
Test Capabilities

Stage Capabilities



TTPs - Mitre ATT&CK

"MITRE's Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK™) is a curated knowledge base and model for cyber adversary behavior, reflecting the various phases of an adversary's lifecycle and the platforms they are known to target"



Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command And Control
10 items	31 items	56 items	28 items	59 items	20 items	19 items	17 items	13 items	9 items	21 items
Drive-by Compromise	AppleScript	.bash_profile and .bashrc	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Account Discovery	AppleScript	Audio Capture	Automated Exfiltration	Commonly Used Port
Exploit Public-Facing Application	CMSTP	Accessibility Features	Accessibility Features	Binary Padding	Bash History	Application Window Discovery	Application Deployment Software	Automated Collection	Data Compressed	Communication Through Removable Media
Hardware Additions	Command-Line Interface	AppCert DLLs	AppCert DLLs	BITS Jobs	Brute Force	Browser Bookmark Discovery	Distributed Component Object Model	Clipboard Data	Data Encrypted	Connection Proxy
Replication Through Removable Media	Control Panel Items	AppInit DLLs	AppInit DLLs	Bypass User Account Control	Credential Dumping	File and Directory Discovery	Exploitation of Remote Services	Data from Information Repositories	Data Transfer Size Limits	Custom Command and Control Protocol
Spearphishing Attachment	Dynamic Data Exchange	Application Shimming	Application Shimming	Clear Command History	Credentials in Files	Network Service Scanning	Logon Scripts	Data from Local System	Exfiltration Over Alternative Protocol	Custom Cryptographic Protocol
Spearphishing Link	Execution through API	Authentication Package	Bypass User Account Control	CMSTP	Credentials in Registry	Network Share Discovery	Pass the Hash	Data from Network Shared Drive	Exfiltration Over Command and Control Channel	Data Encoding
Spearphishing via Service	Execution through Module Load	BITS Jobs	DLL Search Order Hijacking	Code Signing	Exploitation for Credential Access	Password Policy Discovery	Pass the Ticket	Data from Removable Media	Exfiltration Over Other Network Medium	Data Obfuscation
Supply Chain Compromise	Exploitation for Client Execution	Bootkit	Dylib Hijacking	Component Firmware	Forced Authentication	Peripheral Device Discovery	Remote Desktop Protocol	Data Staged	Exfiltration Over Physical Medium	Domain Fronting
Trusted Relationship	Graphical User Interface	Browser Extensions	Exploitation for Privilege Escalation	Component Object Model Hijacking	Hooking	Permission Groups Discovery	Remote File Copy	Email Collection	Scheduled Transfer	Fallback Channels
Valid Accounts	InstallUtil	Change Default File Association	Extra Window Memory Injection	Control Panel Items	Input Capture	Process Discovery	Remote Services	Input Capture		Multi-hop Proxy
	Launchctl	Component Firmware	File System Permissions Weakness	DCShadow	Input Prompt	Query Registry	Replication Through Removable Media	Man in the Browser		Multi-Stage Channels
	Local Job Scheduling	Component Object Model Hijacking	Hooking	Deobfuscate/Decode Files or Information	Kerberoasting	Remote System Discovery	Shared Webroot	Screen Capture		Multiband Communication
	LSASS Driver	Create Account	Image File Execution Options Injection	Disabling Security Tools	Keychain	Security Software Discovery	SSH Hijacking	Video Capture		Multilayer Encryption
	Mshta	DLL Search Order Hijacking	Launch Daemon	DLL Search Order Hijacking	LLMNR/NBT-NS Poisoning	System Information Discovery	Taint Shared Content			Port Knocking
	PowerShell	Dylib Hijacking	New Service	DLL Side-Loading	Network Sniffing	System Network Configuration Discovery	Third-party Software			Remote Access Tools
	Regsvcs/Regasm	External Remote Services	Path Interception	Exploitation for Defense Evasion	Password Filter DLL	System Network Connections Discovery	Windows Admin Shares			Remote File Copy
	Regsvr32	File System Permissions Weakness	Plist Modification	Extra Window Memory Injection	Private Keys	System Owner/User Discovery	Windows Remote Management			Standard Application Layer Protocol
	Rundll32	Hidden Files and Directories	Port Monitors	File Deletion	Replication Through Removable Media	System Service Discovery				Standard Cryptographic Protocol
	Scheduled Task	Hooking	Process Injection	File System Logical Offsets	Securityd Memory					Standard Non-Application Layer Protocol
	Scripting	Hypervisor	Scheduled Task	Gatekeeper Bypass	Two-Factor Authentication Interception					Uncommonly Used Port
	Service Execution	Image File Execution Options Injection	Service Registry Permissions Weakness	Hidden Files and Directories						Web Service
	Signed Binary Proxy Execution	Kernel Modules and Extensions	Setuid and Setgid	Hidden Users						
	Signed Script Proxy Execution	Launch Agent		Hidden Window						
	Source			HISTCONTROL						
	Space after Filename			Image File Execution Options Injection						

Analysis

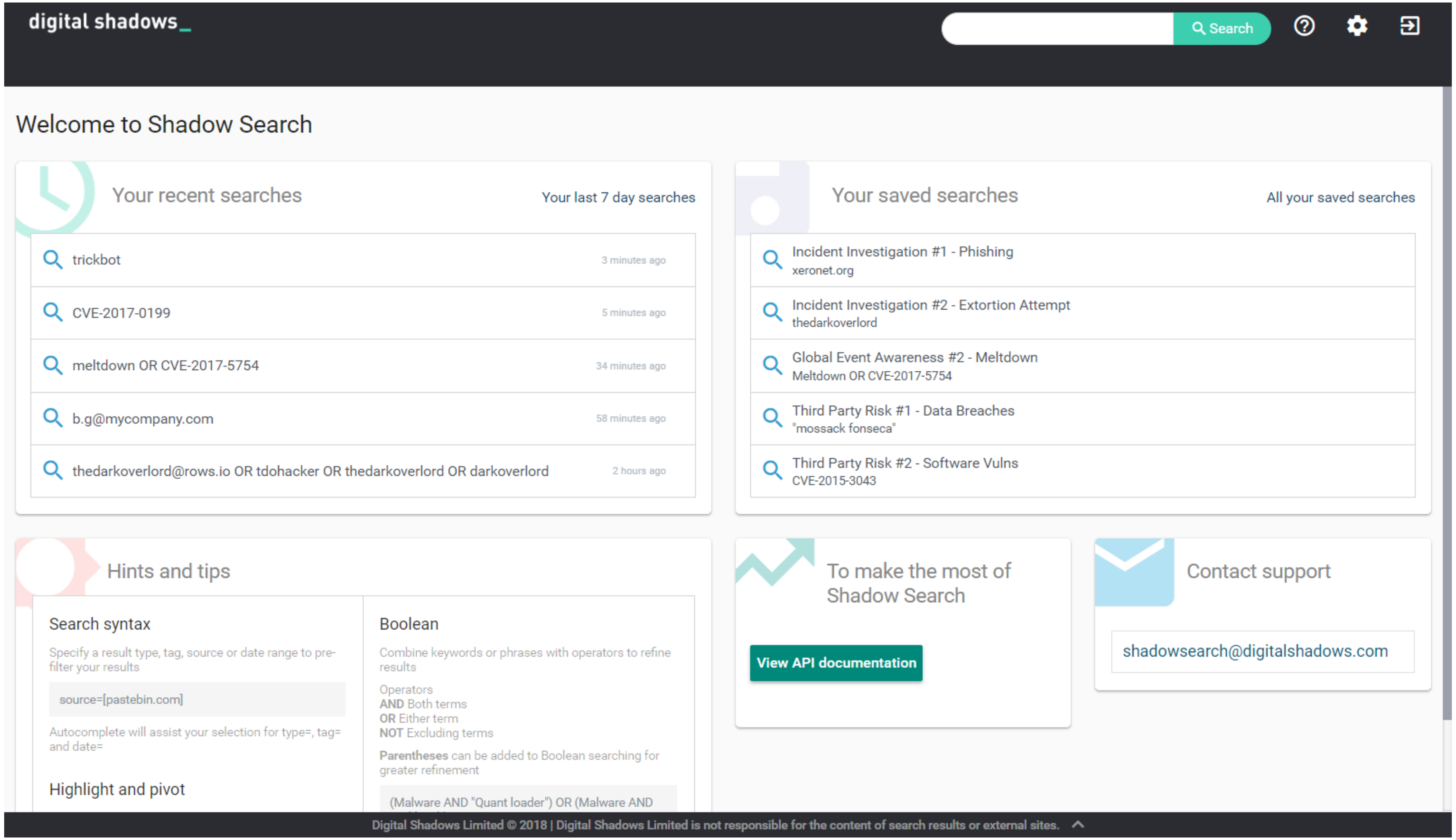
- Data Enrichment
  - Free services: Virus Total, Domain tools, Passive Total, OTX
  - Commercial Services: Shadow Search, Recorded Future
  - Threat sharing platforms: MISP, STIX

  - Objective: Provide context to the investigated data – IOCs

  - An extensive list here: https://www.prodefence.org/most-important-cyber-threat-intelligence-tools-list-for-hackers-and-security-professionals/

Advanced Search and Investigation

- Shadow Search: an example of an advanced Threat Intelligence investigation service



Welcome to Shadow Search

Your recent searches — Your last 7 day searches

trickbot	3 minutes ago
CVE-2017-0199	5 minutes ago
meltdown OR CVE-2017-5754	34 minutes ago
b.g@mycompany.com	58 minutes ago
thedarkoverlord@rows.io OR tdohacker OR thedarkoverlord OR darkoverlord	2 hours ago

Your saved searches — All your saved searches

- Incident Investigation #1 - Phishing
xeronet.org
- Incident Investigation #2 - Extortion Attempt
thedarkoverlord
- Global Event Awareness #2 - Meltdown
Meltdown OR CVE-2017-5754
- Third Party Risk #1 - Data Breaches
"mossack fonseca"
- Third Party Risk #2 - Software Vulns
CVE-2015-3043

Hints and tips

Search syntax

Specify a result type, tag, source or date range to pre-filter your results

source=[pastebin.com]

Autocomplete will assist your selection for type=, tag= and date=

Highlight and pivot

Boolean

Combine keywords or phrases with operators to refine results

Operators
AND Both terms
OR Either term
NOT Excluding terms

Parentheses can be added to Boolean searching for greater refinement

(Malware AND "Quant loader") OR (Malware AND

To make the most of Shadow Search

View API documentation

Contact support

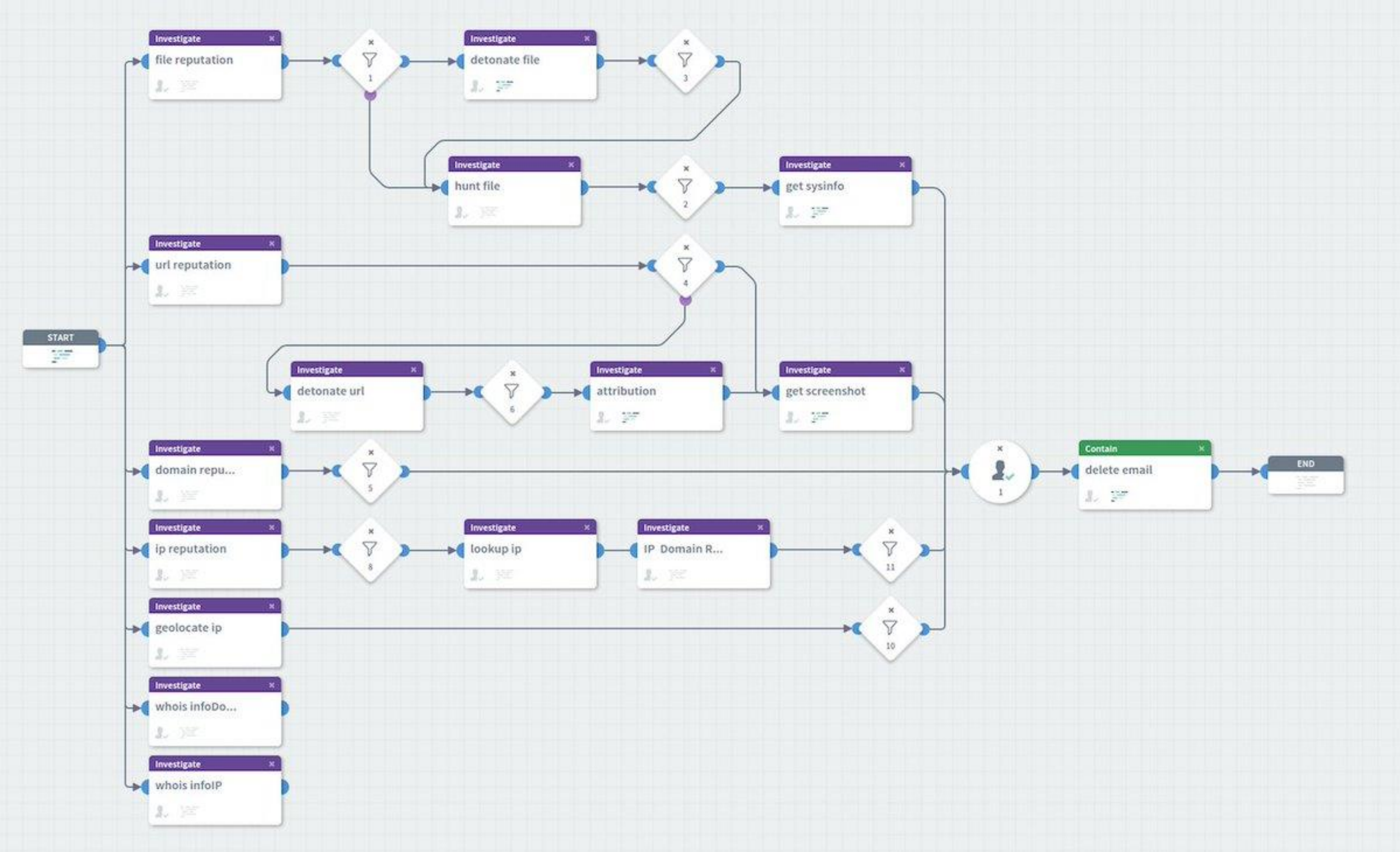
shadowsearch@digitalshadows.com

Digital Shadows Limited © 2018 | Digital Shadows Limited is not responsible for the content of search results or external sites.

Explore and interpret the data using Timeline View or Summary View along with detail screens

Automation

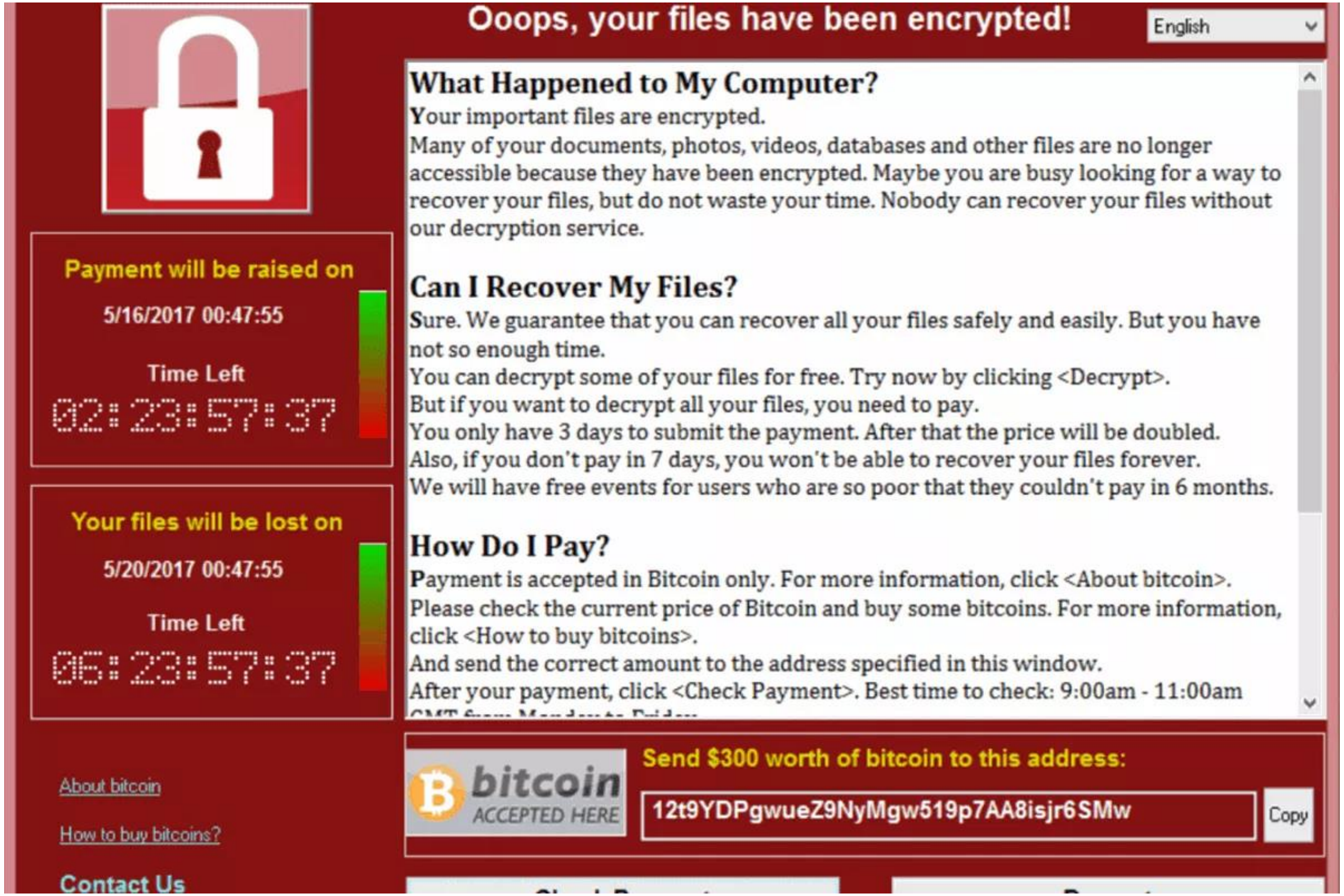
- Cyber Phantom: Incident response automation, IOC investigation use case



Containment

Containment	
Incident Response	**Threat Intelligence**
Stopping the spread	Apply identified malicious IPs and URLs
Prevent further damage	Apply public threat lists
Disabling services	
Disabling connectivity	

Ransomware



Ooops, your files have been encrypted!

Payment will be raised on

5/16/2017 00:47:55

Time Left

02:23:57:37

Your files will be lost on

5/20/2017 00:47:55

Time Left

06:23:57:37

What Happened to My Computer?

Your important files are encrypted.

Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

Can I Recover My Files?

Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.

You can decrypt some of your files for free. Try now by clicking <Decrypt>.

But if you want to decrypt all your files, you need to pay.

You only have 3 days to submit the payment. After that the price will be doubled.

Also, if you don't pay in 7 days, you won't be able to recover your files forever.

We will have free events for users who are so poor that they couldn't pay in 6 months.

How Do I Pay?

Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.

Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.

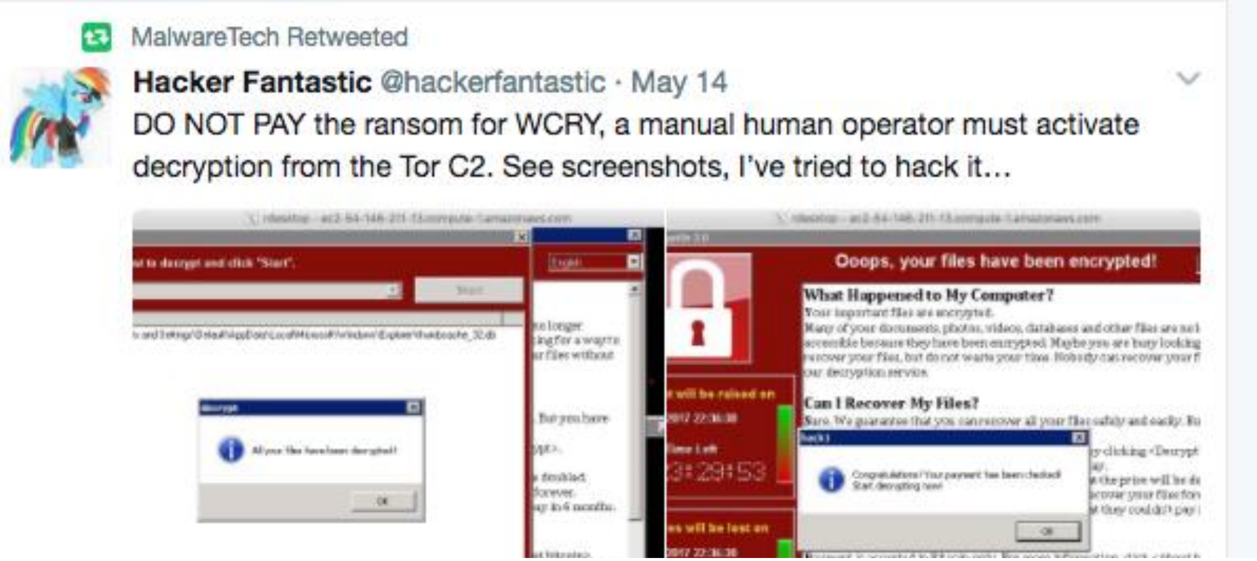
And send the correct amount to the address specified in this window.

After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am

Send $300 worth of bitcoin to this address:

12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw

Public recommendations



MalwareTech Retweeted

Hacker Fantastic @hackerfantastic · May 14

DO NOT PAY the ransom for WCRY, a manual human operator must activate decryption from the Tor C2. See screenshots, I've tried to hack it...

...t to decrypt and click "Start".

All your files have been decrypted!

Ooops, your files have been encrypted!

What Happened to My Computer?

Your important files are encrypted.

Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

Can I Recover My Files?

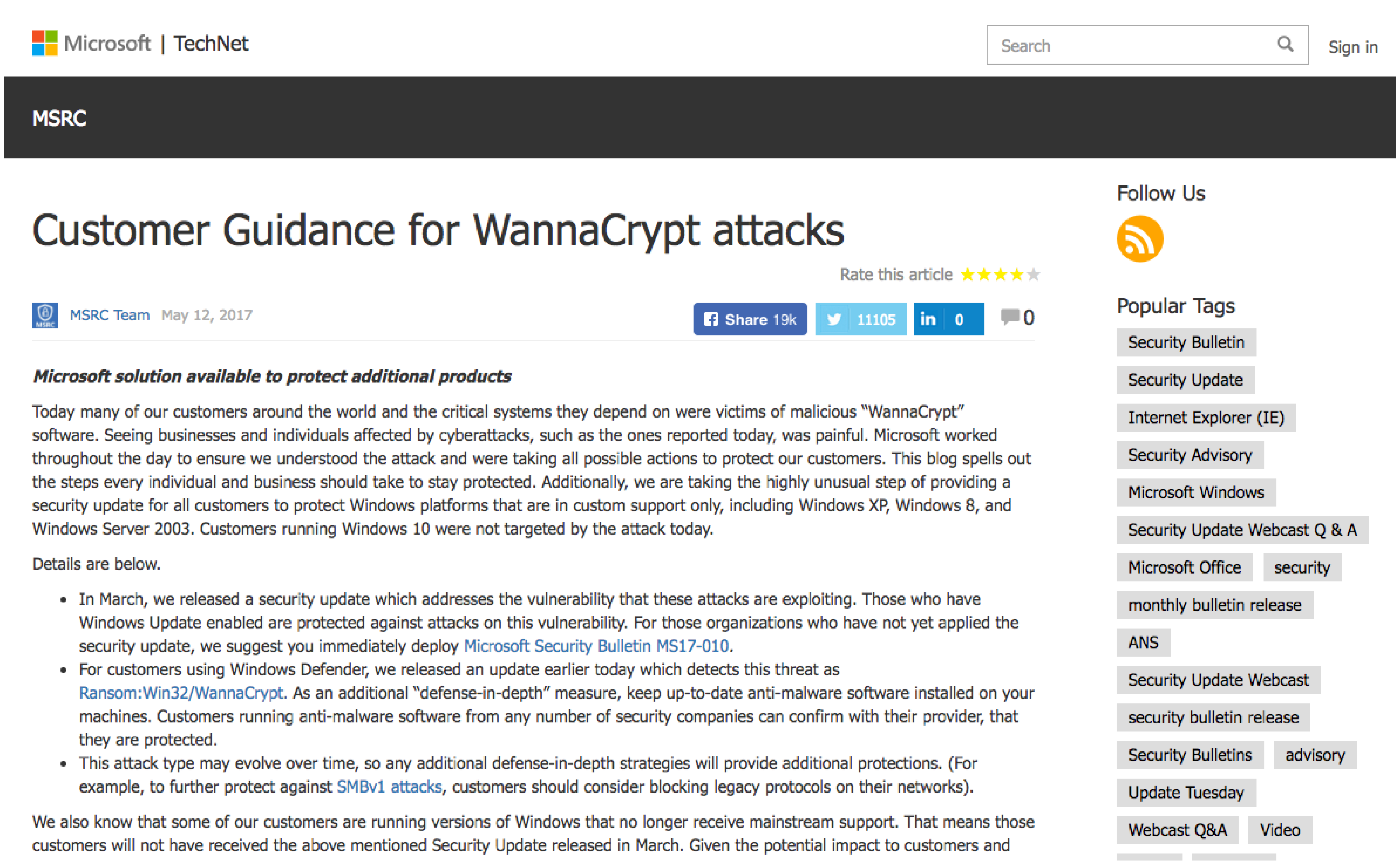
Sure. We guarantee that you can recover all your files safely and easily. Bu...

Congratulations! Your payment has been checked!
Start decrypting now!

The NCSC's latest statement on the international ransomware cyber incident ❯

The NCSC's latest statement on the international ransomware cyber attack

Specific guidance



Customer Guidance for WannaCrypt attacks

Rate this article ★★★★☆

MSRC Team May 12, 2017

Microsoft solution available to protect additional products

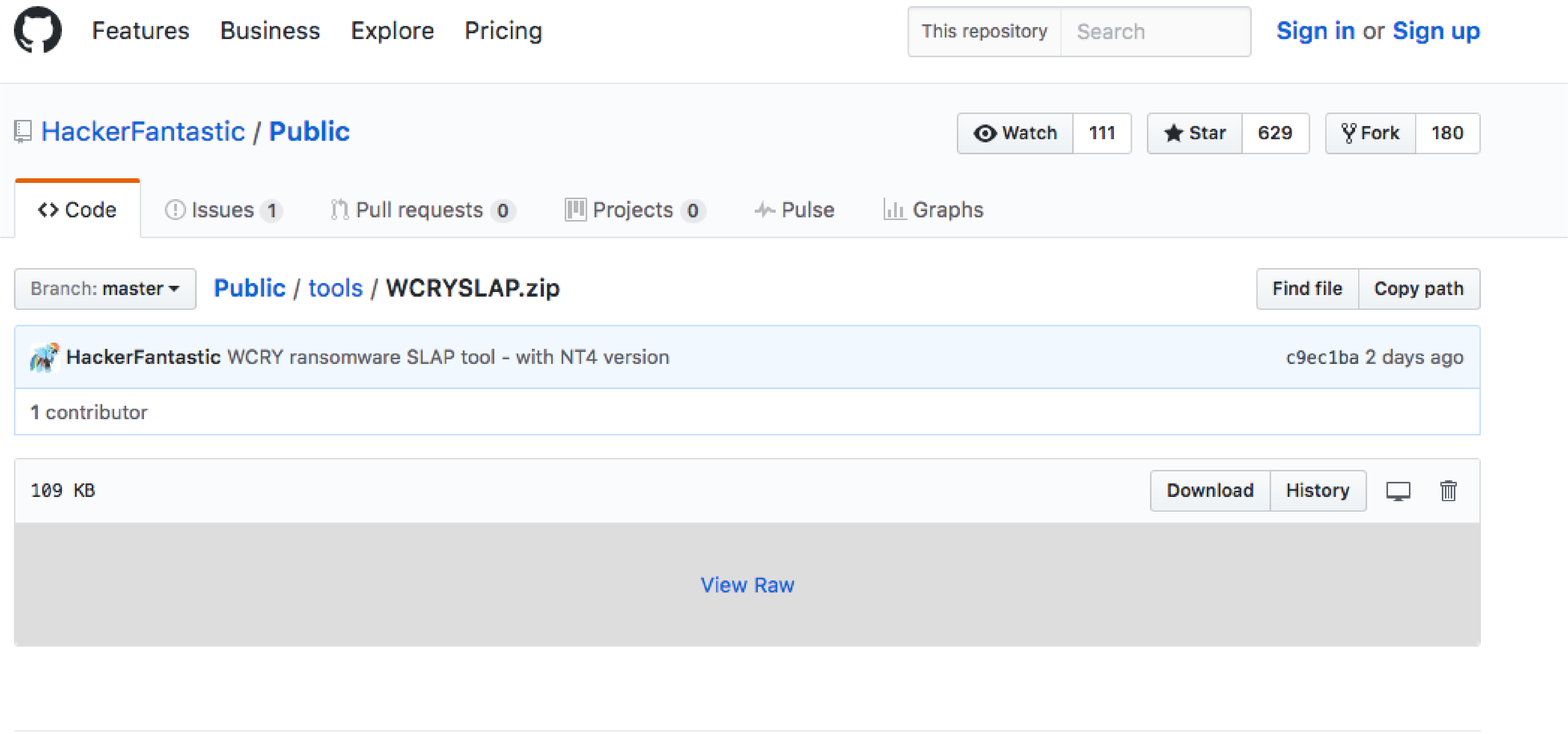
Today many of our customers around the world and the critical systems they depend on were victims of malicious "WannaCrypt" software. Seeing businesses and individuals affected by cyberattacks, such as the ones reported today, was painful. Microsoft worked throughout the day to ensure we understood the attack and were taking all possible actions to protect our customers. This blog spells out the steps every individual and business should take to stay protected. Additionally, we are taking the highly unusual step of providing a security update for all customers to protect Windows platforms that are in custom support only, including Windows XP, Windows 8, and Windows Server 2003. Customers running Windows 10 were not targeted by the attack today.

Details are below.

- In March, we released a security update which addresses the vulnerability that these attacks are exploiting. Those who have Windows Update enabled are protected against attacks on this vulnerability. For those organizations who have not yet applied the security update, we suggest you immediately deploy Microsoft Security Bulletin MS17-010.
- For customers using Windows Defender, we released an update earlier today which detects this threat as Ransom:Win32/WannaCrypt. As an additional "defense-in-depth" measure, keep up-to-date anti-malware software installed on your machines. Customers running anti-malware software from any number of security companies can confirm with their provider, that they are protected.
- This attack type may evolve over time, so any additional defense-in-depth strategies will provide additional protections. (For example, to further protect against SMBv1 attacks, customers should consider blocking legacy protocols on their networks).

We also know that some of our customers are running versions of Windows that no longer receive mainstream support. That means those customers will not have received the above mentioned Security Update released in March. Given the potential impact to customers and

Tools



HackerFantastic / Public

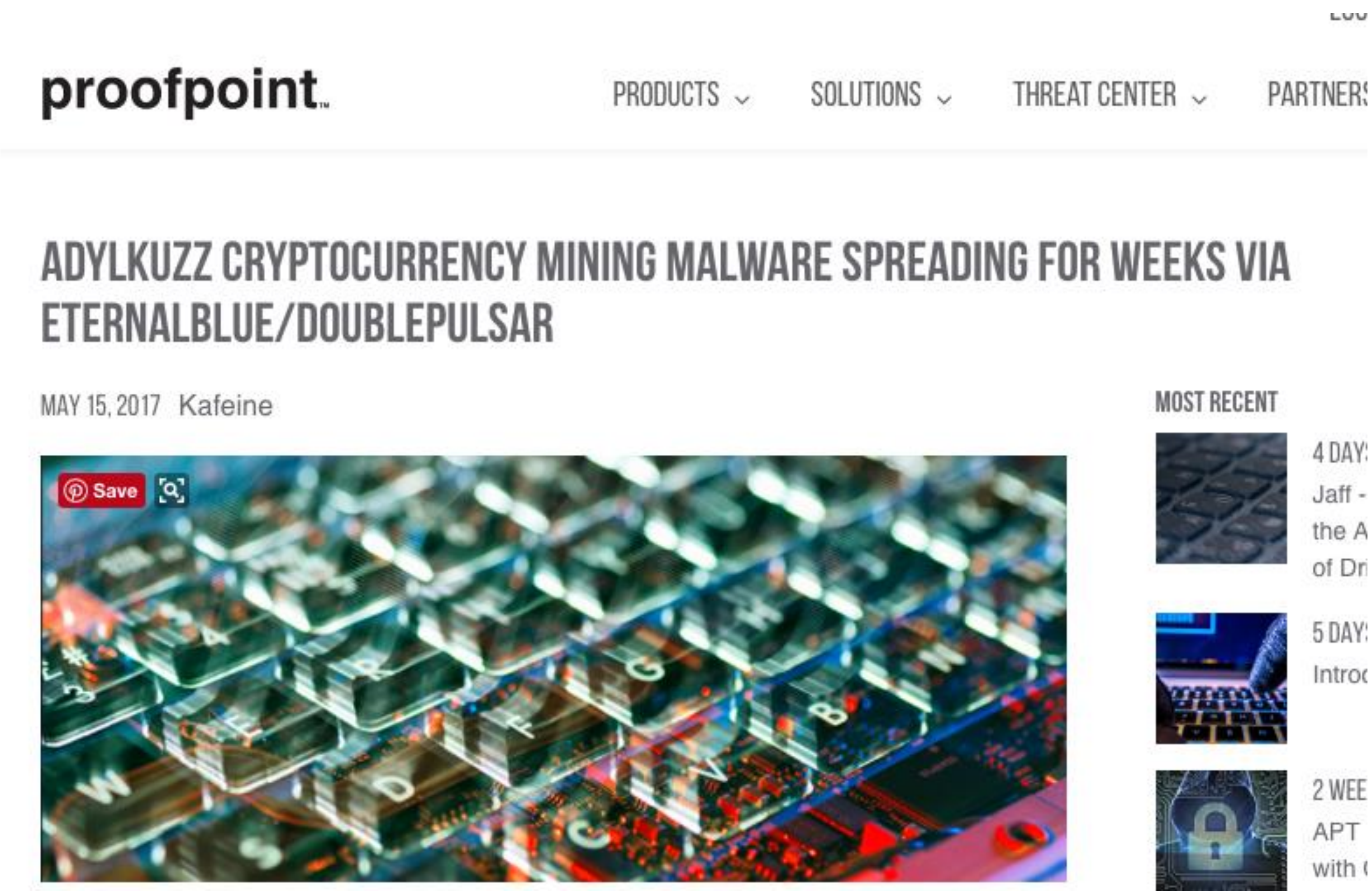
Public / tools / WCRYSLAP.zip

HackerFantastic WCRY ransomware SLAP tool - with NT4 version c9ec1ba 2 days ago

1 contributor

109 KB

Port 445 EternalBlue/DoublePulsar exclusive to WannCrypt?



proofpoint.

PRODUCTS ⌄ SOLUTIONS ⌄ THREAT CENTER ⌄ PARTNERS

ADYLKUZZ CRYPTOCURRENCY MINING MALWARE SPREADING FOR WEEKS VIA ETERNALBLUE/DOUBLEPULSAR

MAY 15, 2017 Kafeine

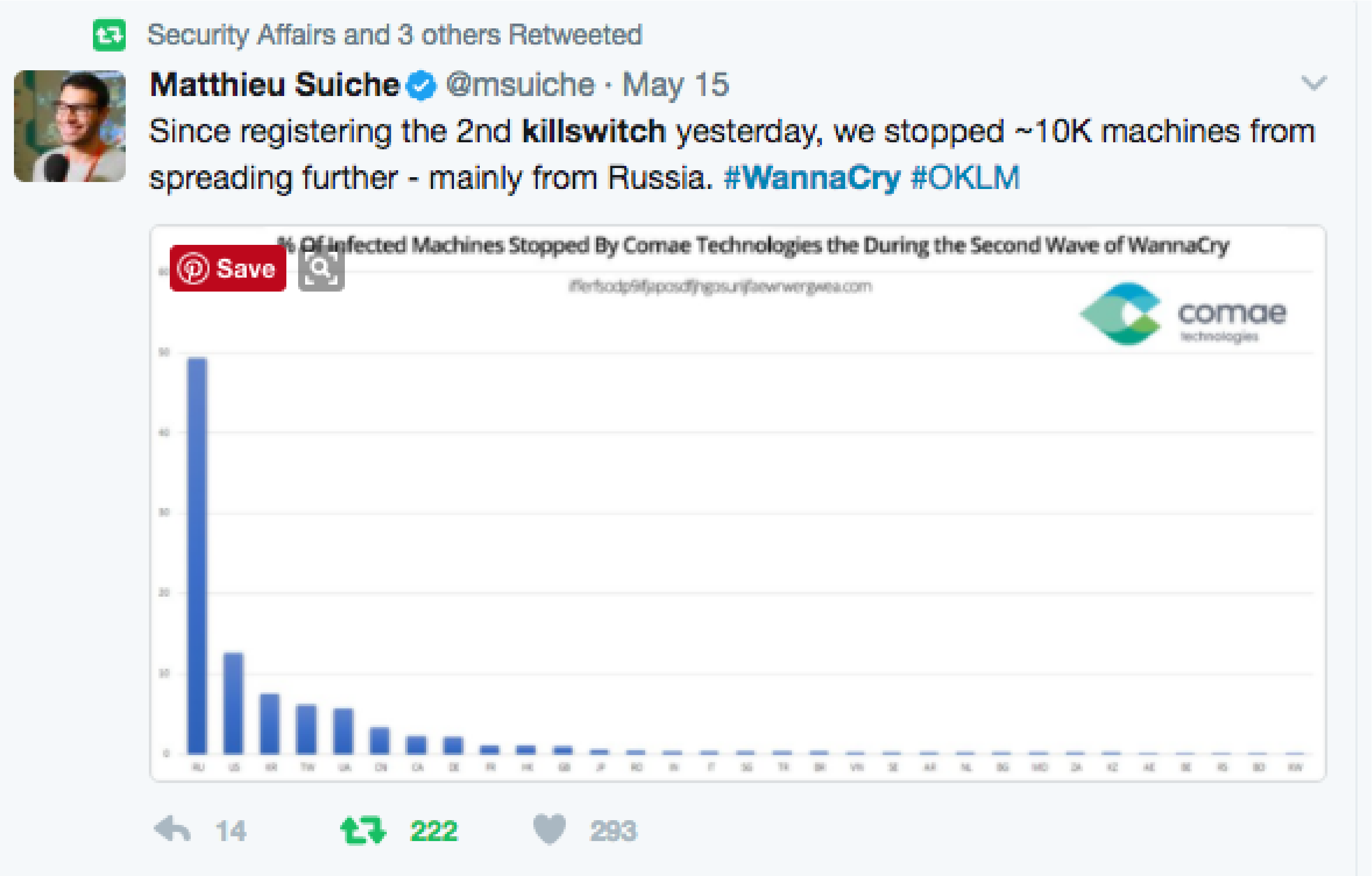
MOST RECENT

4 DAY
Jaff -
the A
of Dr

5 DAY
Introd

2 WEE
APT
with

Sharing



Security Affairs and 3 others Retweeted

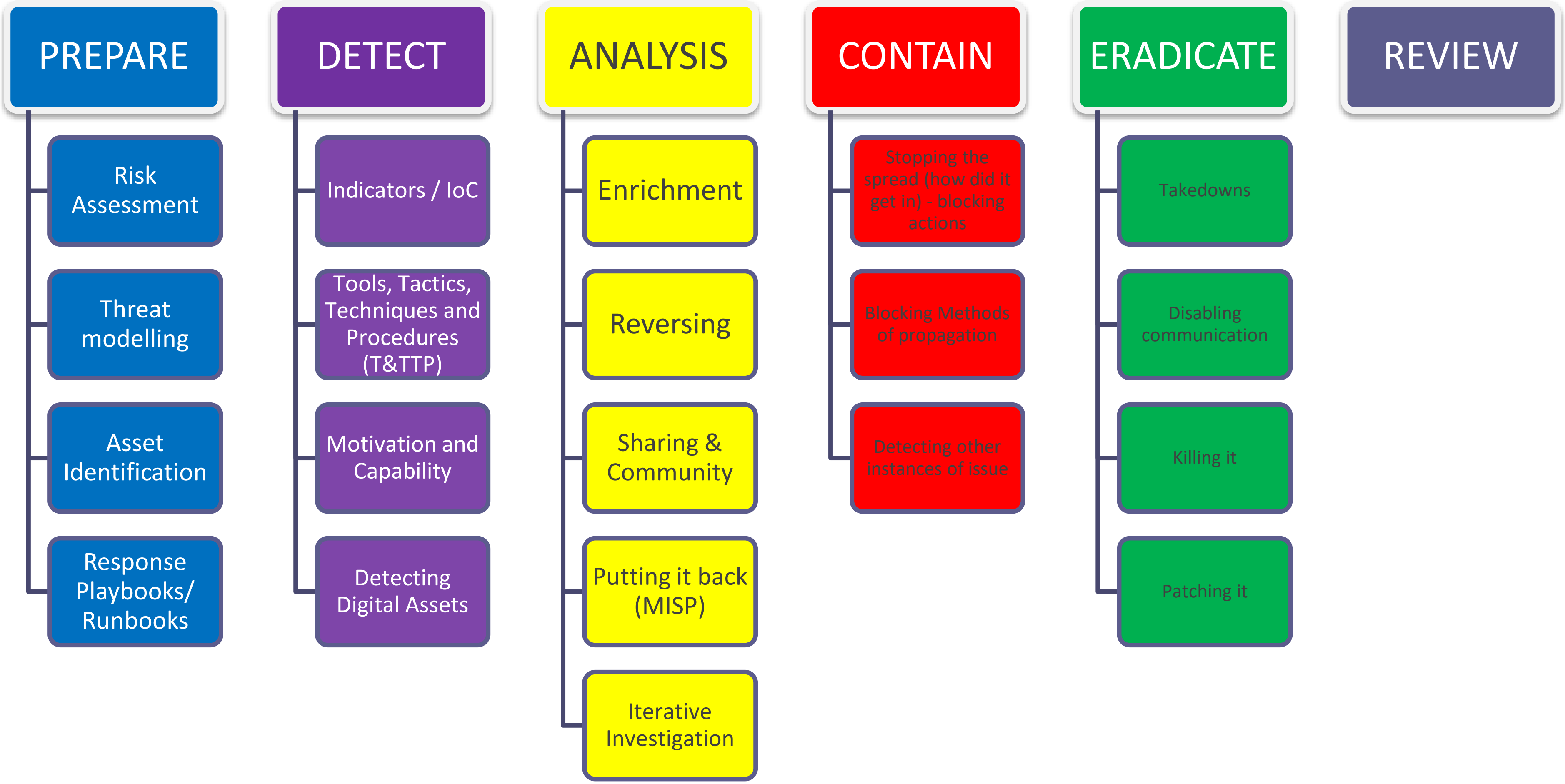
Matthieu Suiche @msuiche · May 15

Since registering the 2nd **killswitch** yesterday, we stopped ~10K machines from spreading further - mainly from Russia. #WannaCry #OKLM

% Of Infected Machines Stopped By Comae Technologies the During the Second Wave of WannaCry
ifferfsodp9ifjaposdfjhgosurijfaewrwergwea.com
comae technologies
Save
60
50
40
30
20
10
0
RU
US
KR
TW
UA
CN
CA
DE
FR
HK
GB
JP
RO
IN
IT
SG
TR
BR
VN
SE
AR
NL
BG
MD
ZA
KZ
AE
BE
RS
BD
KW
14
222
293

Post Incident Activity	
Incident Response	**Threat Intelligence**
Lessons Learned	
Improve the process	

A Process for incident management



PREPARE

- Risk Assessment
- Threat modelling
- Asset Identification
- Response Playbooks/ Runbooks

DETECT

- Indicators / IoC
- Tools, Tactics, Techniques and Procedures (T&TTP)
- Motivation and Capability
- Detecting Digital Assets

ANALYSIS

- Enrichment
- Reversing
- Sharing & Community
- Putting it back (MISP)
- Iterative Investigation

CONTAIN

- Stopping the spread (how did it get in) - blocking actions
- Blocking Methods of propagation
- Detecting other instances of issue

ERADICATE

- Takedowns
- Disabling communication
- Killing it
- Patching it

REVIEW

Conlusions - Takeaways

- CTI – We already do it/ did it, part of the entire Incident Response process
- BUT there are new opportunities and innovation
- It’s part of forensic discipline, but trying to get earlier in the chain
- It applies well to the earlier stages of the incident lifecycle and best focused
- Indicators can be useful, but ephemeral, fragile and incomplete
- TTP’s can have longer lasting value but require much more effort to acquire and develop
- Sharing and clear communication is at the center
- This will continue to develop

www.digitalshadows.com

London

7 Westferry Circus, Columbus Building, Level 6
London E14 4HD

T: +44 (0)203 393 7001

✉ info@digitalshadows.com

San Francisco

332 Pine St. Suite 600
San Francisco, CA 94104

T: +1 888 889-4143

Dallas

5307 Mockingbird Lane, Suite 200
Dallas, TX 95206

digital shadows_