



Adversarial Threat Modelling: A Practical Approach to Purple Teaming in the Enterprise

NOVEMBER 2021
Sajid Nawaz Khan

PUBLIC

HELLO

WELCOME TO THE WORKSHOP



Thank you for joining my workshop today, it's a pleasure to be presenting at Becks JP.

whoami

- Sajid Nawaz Khan
- In finance sector 15+ years
- Senior Cyber Threat Intelligence Analyst, five years in security
- GIAC GREM, GDAT certified
- Mitre ATT&CK evangelist

/etc

Food, films, museums, science, origami and more.

WORKSHOP AGENDA

OUR PLAN TODAY

1

Presentation · 1 HOUR

The problem, and our approach to intelligence-led Purple Teaming

2

Demo · 15 MINS

A practical demonstration of VECTR; for analysts *and* managers

3

Questions · 15 MINS

An opportunity to ask questions about our approach

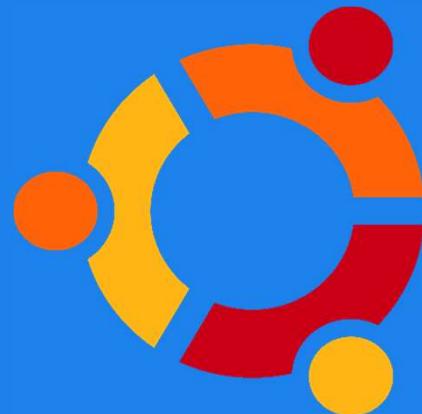


REQUIREMENTS

PREPARING FOR SUCCESS



VirtualBox or equivalent, with Extension Pack, Guest Additions and fast internet connectivity



Ubuntu 20.04.1 LTS, with 4GB RAM, 20GB disk space and bi-directional clipboard and file sharing



VECTR, please follow the installation guide including dependencies at docs.vectr.io

IT'S BEEN A BUSY YEAR

LITTLE REST FOR DEFENDERS

January

Hackers launch ransomware attacks against five major gaming and gambling countries, demanding over \$100 million in ransom.

Unidentified hackers breached one of the data centers of New Zealand's central bank.

Hackers active since 2012 attack business and governments across South and East Asia, with a particular emphasis on military and government organizations in Pakistan, China, Nepal, and Afghanistan, and businesses involved in defence technology, scientific research, finance, energy, and mining.

North Korean government hackers engaged in a sophisticated social engineering campaign against cybersecurity researchers that used multiple fake twitter accounts and a fake blog to drive targets to infected sites or induce them to open infected attachments in emails asking the target to collaborate on a research project.

Hackers linked to Hezbollah breached telecom companies, internet service providers, and hosting providers in the US, UK, Egypt, Israel, Lebanon, Jordan, Saudi Arabia, the UAE, and the Palestinian Authority for intelligence gathering and data theft.

February

Two Iranian hacking groups conducted espionage campaigns against Iranian dissidents in sixteen countries in the Middle East, Europe, South Asia, and North America.

Unknown hackers attempted to raise levels of sodium hydroxide in the water supply of Oldsmar, Florida by a factor of 100 by exploiting a remote access system.

North Korean hackers attempted to break into the computer systems of pharmaceutical company Pfizer to gain information about vaccines and treatments for the COVID-19.

Source



Center for Strategic & International Studies (CSIS)

www.csis.org/programs/technology-policy-program/significant-cyber-incidents

IT'S BEEN A BUSY YEAR

LITTLE REST FOR DEFENDERS

SOURCE: CSIS

March

Ukraine's State Security Service announced it had prevented a large-scale attack by Russian FSB hackers attempting to gain access to classified government data.

The head of U.S. Cyber Command testified that the organization had conducted more than two dozen operations to confront foreign threats ahead of the 2020 U.S. elections, including eleven forward hunt operations in nine different countries.

Suspected Russian hackers attempted to gain access to the personal email accounts of German parliamentarians in the run-up to Germany's national elections.

April

The European Commission announced that the EC and multiple other EU organizations were hit by a major cyberattack by unknown hackers.

MI5 warned that over 10,000 UK professionals have been targeted by hostile states over the past five years as part of spearphishing and social engineering campaigns on LinkedIn.

Two state-backed hacking groups exploit vulnerabilities in a VPN service to target organizations across the U.S. and Europe.

Malware triggered an outage for airline reservation systems that caused the networks of 20 low-cost airlines around the world to crash.

May

A large DDoS attack disabled the ISP used by Belgium's government, impacting more than 200 organizations causing the cancellation of multiple Parliamentary meetings.

On May 6, the Colonial Pipeline, the largest fuel pipeline in the United States, was the target of a ransomware attack. The energy company shut down the pipeline and later paid a \$5 million ransom. The attack is attributed to DarkSide, a Russian speaking hacking group.

On May 24th, hackers gained access to Fujitsu's systems and stole files belonging to multiple Japanese government entities. So far four government agencies have been impacted.

IT'S BEEN A BUSY YEAR

LITTLE REST FOR DEFENDERS

SOURCE: CSIS

June

A spreadsheet was leaked containing classified personal details of the 1,182 United Kingdom's Special Forces soldier.

Hackers linked to Russia's Foreign Intelligence Service installed malicious software on a Microsoft system that allowed hackers to gain access to accounts and contact information. The majority of the customers targeted were U.S. based, working for IT companies or the government.

The Iranian government launched a widespread disinformation campaign, targeting WhatsApp groups, Telegram channels and messaging apps used by Israeli activists. The campaign aimed to advance political unrest and distrust in Israel.

July

Russian hackers exploited a vulnerability in Kaseya's virtual systems/server administrator (VSA) software allowing them to deploy a ransomware attack on the network. The hack affected around 1,500 small and midsized businesses.

Several countries used Pegasus, surveillance software created by NSO Group that targets iPhone and Android operating systems, on devices belonging to activists, politicians, and journalists.

A cyberattack gained access to 1 terabyte of data from the Saudi Arabian Oil Company through a zero-day exploitation. Hackers are offering to delete the data in exchange for \$50 million in cryptocurrency.

August

A cyberattack on the Covid-19 vaccine-scheduling website for the Italian region of Lazio forced the website to temporarily shut down. New vaccination appointments were unable to be scheduled for several days after the attack.

A cyber-espionage group linked to one of Russia's intelligence forces targeted the Slovak government from February to July 2021 through spear-fishing attempts.

A cyberattack on the government of Belarus compromised dozens of police and interior ministry databases. The hack claims to be a part of an attempt to overthrow President Alexander Lukashenko's regime.

IT'S BEEN A BUSY YEAR

LITTLE REST FOR DEFENDERS

SOURCE: CSIS

September

The Norwegian Government stated a series of cyberattacks against private and state IT infrastructure came from bad actors operating from China. Their investigation of the hacks claims the actors attempted to capture classified information relating to Norway's national defence and security intelligence.

Hackers obtained 15 TB of data from 8,000 organizations working with Israel-based company, Voicenter and offered the data online for \$1.5 million. Some experts have stipulated the hackers have ties to Iran, but no link has been confirmed.

October

An American company announced that the Russian Foreign Intelligence Service (SVR) launched a campaign targeting resellers and other technology service providers that customize, deploy and manage cloud services.

A group with ties to Iran attempted to hack over 250 Office 365 accounts. All the targeted accounts were either U.S. and Israeli defence technology companies, had a focus on Persian Gulf ports of entry, or maritime transportation companies with a presence in the Middle East.

Hackers leaked data and photos from the Israeli Defence Ministry after gaining access to 165 servers and 254 websites, overall compiling around 11 terabytes of data.

November

An online stock trading platform has confirmed that hackers obtained personal information of more than seven million of its customers. Robinhood, which is available only to U.S. users, said in a blog that hackers "socially engineered" a customer support employee and obtained access to certain customer support systems.

A presentation by Mandiant at the Black Hat Europe conference reported a rise in cyber attacks targeting virtual private networks (VPNs). The rise corresponds with the increased use of VPNs for remote working.

...

THREAT LANDSCAPE

UNDERSTANDING THE ADVERSARY



Increase in sophistication and resources



LONE WOLF · INSIDER

Often opportunistic. Tooling, capabilities and motivations vary

Ready Made Tools



HACKTIVISTS · TERRORISTS

Ideological activism; disruption of services or access. Often funded

DDoS Propaganda



ORGANISED CRIMINALS

Financially motivated. Use of commodity malware, phishing etc

Social Engineering Malware Mules

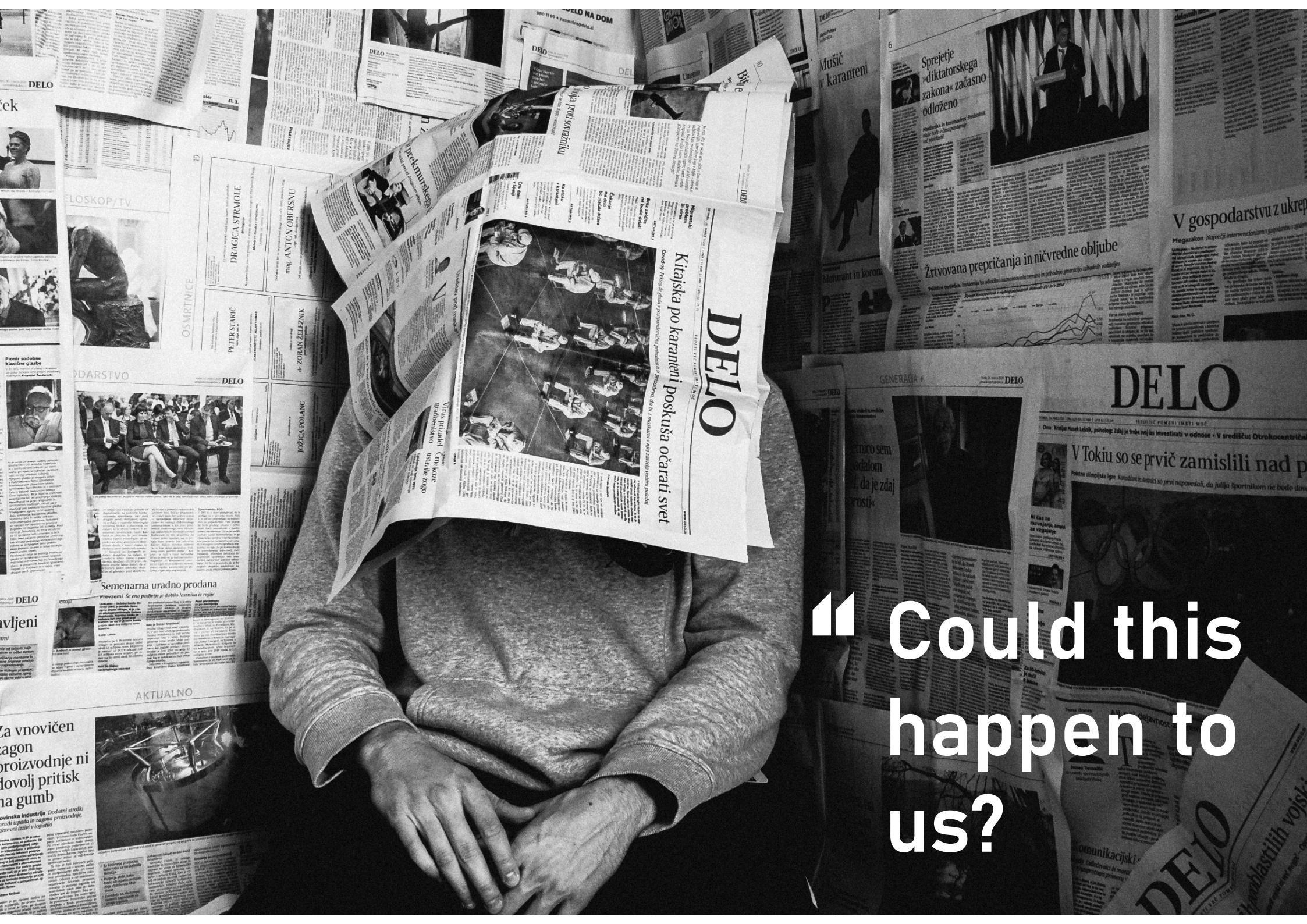


NATION STATE · APTs

IP theft, cyber espionage. Very capable and well resourced threat actor

Zero Days Custom Tooling Patience
Supply Chain Surveillance

“ Could this
happen to
us? ”



“ Could
this
happen
to us?

BEFORE

- “ ... defence in depth
- ... indicators ingested
- ... industry-leading controls
- ... visibility via peers and industry trust groups
- ... couldn't / wouldn't happen to us

...

“ Could
this
happen
to us?

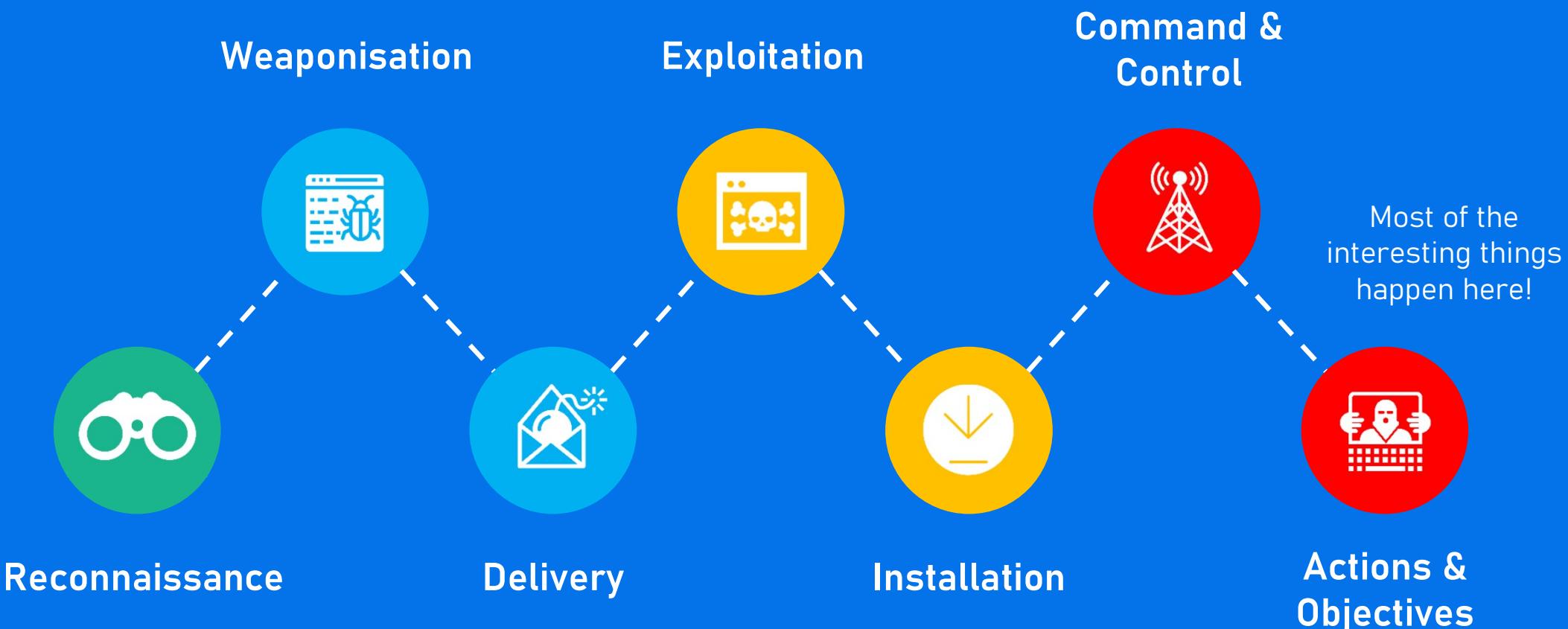
AFTER

” Threat Intelligence are aware of *7 Tier One actors*, including *Lazarus*, using *Techniques A, B, C* in a number of successful attacks within the sector.

We therefore *strongly recommend* developing and deploying *Control X* as a priority; to detect and mitigate any impact from this technique.

HOW DID WE GET HERE?

MOVING BEYOND THE LOCKHEED MARTIN KILL CHAIN



Enterprise ATT&CK (14→218)

Phases Techniques

MITRE NAVIGATOR

VISUALISE THE ADVERSARY

The Mitre Navigator can be used to highlight techniques used by specific adversaries, create heat maps for heavily used techniques, or visualise your defensive coverage

Lazarus x +

selection controls layer controls technique controls

MITRE ATT&CK® Navigator ?

Initial Access	Execution	Persistence	Defense Evasion	Discovery	Collection	Command and Control	Exfiltration	Impact
1 techniques	2 techniques	1 techniques	1 techniques	8 techniques	2 techniques	3 techniques	1 techniques	4 techniques
Drive-by Compromise	Exploitation for Client Execution	Account Manipulation (0/0)	Obfuscated Files or Information (0/0)	Application Window Discovery	Archive Collected Data (0/2)	Fallback Channels	Exfiltration Over C2 Channel	Data Destruction
	Windows Management Instrumentation			File and Directory Discovery	Data from Local System	Ingress Tool Transfer		Resource Hijacking
				Process Discovery		Non-Standard Port		Service Stop
				Query Registry				System Shutdown/Reboot
				System Information Discovery				
				System Network Configuration Discovery				
				System Owner/User Discovery				
				System Time Discovery				

MITRE ATT&CK® Navigator v3.1

IS MITRE ATT&CK ENOUGH?

MORE DETAIL == BETTER DECISIONS



Techniques & sub-techniques still don't often provide enough detail to replicate an attack †



Mitre knowledgebase is extensive, but only includes public information, which may not reflect reality



Techniques are not always distilled to individual toolkits or intrusions, so harder to identify trends

† GRANULAR PROCEDURE LEVEL INFORMATION IS IN THE MITRE ROADMAP

PHISHING · T1566

HOW MANY WAYS CAN YOU THINK OF?



Macro
Cobalt Strike
Standard



Macro
Cobalt Strike
Standard as HREF



Macro
Cobalt Strike
as URL Rewrite



Macro
WScript
PowerShell



Macro
Wscript
leading to EXE



Macro
WScript
PowerShell XOR



Macro
MMG WMI
PowerShell



Macro LuckyStrike
PowerShell
CellEmbed



Macro
MSBuild



DDE
PowerShell



Macro
Remote
Template



Encrypted
Archive



Password
Protected
Office Doc



Link
Inside
PDF



Link
Inside Office
Document



File:
HTA



File:
EXE



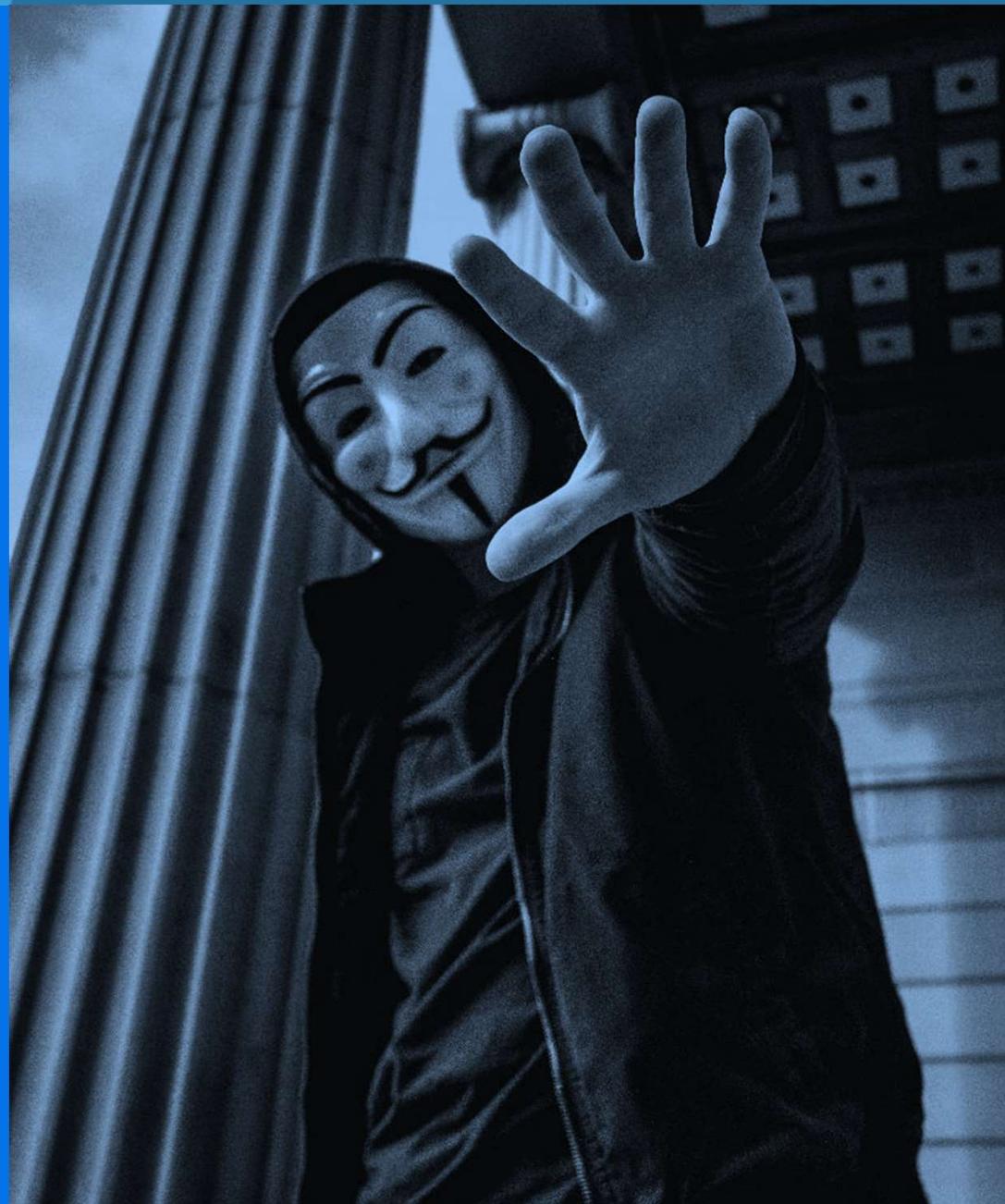
File:
.BAT

BECOMING THREAT-LED

AN ADVERSERIAL APPROACH TO PURPLE TEAMING

What We Wanted to Achieve

- List of threat actors, associated campaigns and TTPs of interest to Standard Chartered and the Financial Services industry
- Granular level understanding of TTPs, and how specifically these can be detected and blocked in our environment
- Remove control-efficacy ambiguity from TTPs, and provide confidence and assurance that controls are effective, through atomic level testing
- A library of TTPs aligned to the Mitre Enterprise framework, which would be actively maintained by Threat Intelligence and security teams



BECOMING THREAT-LED

INTEGRATING INTELLIGENCE IN YOUR APPROACH

Using Threat Intelligence can bring focus to Purple Team initiatives, helping to prioritise those Threat Actors and TTPs that are likely to be the greatest threat to your organisation and technology stack. Your Cyber Threat Intelligence team will work with internal stakeholders, peers, trust groups and vendors to develop a detailed understanding of the threat landscape. Mitre's *Level 3* approach is detailed below:

ADVERSARY EMULATION PLAN



Gather
threat intelligence
based on the
threats to your
organisation

Extract
techniques and
map to your
preferred
framework

Analyse
, organise and
diagram your
analysis into an
operational flow

Develop
tools and
procedures to help
teams replicate
the attack

Emulate
the adversary,
working closely
with Blue Teams
to identify gaps

Essential Reading

medium.com/mitre-attack/getting-started-with-attack-red-29f074ccf7e3
medium.com/mitre-attack/getting-started-with-attack-cti-4eb205be4b2f

OUR APPROACH

TPP CENTRIC, FOCUSING ON SPECIFIC INTRUSIONS

THREAT-LED



Focus on TPPs

Our focus is on the top two tiers of the Pyramid of Pain



Threat Actor

Understanding which adversaries are the greatest risk



Cyber Attack

Prominent cyber attack or tool used by the adversary



Specific TTP

Specific way a tool was used by the adversary

LAZARUS

BANK OF BANGLADESH

TTP 1

FAR EASTERN INTERNATIONAL BANK

TTP 2

TROY OPERATION

TTP 3

DARKSEOUL OPERATION

TTP 4

SONY PICTURES

ETC

Malpedia and the Thai CERT Threat Actor Encyclopedia are a great place to start:

- malpedia.caad.fkie.fraunhofer.de/actors
- apt.thaicert.or.th/cgi-bin/listgroups.cgi

OUR APPROACH

OPERATIONALISING THREAT INTELLIGENCE

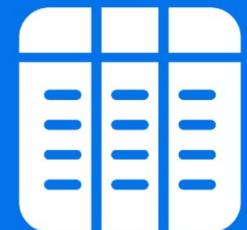
We wanted to industrialise the end-to-end pipeline between Threat Intelligence, Purple Teams, Detection Engineering, Threat Hunting and finally, Red/Blue teams for validation.

Threat Intelligence



Research

Understanding the Threat Landscape and attacks to the Finance sector



Map

Breaking down known TTPs to specific Mitre Intrusion Sets

Purple Team, Detection Engineering



Assess

Identifying how these TTPs might be detected via current controls



Enhance

Improving and prioritising detection capabilities

Red & Blue Teams



Validate

Testing efficacy of controls and TTP detection via Red Teaming

OUR APPROACH

SME THOUGHT PROCESS

Which specific threat actors (or intrusion sets) are the greatest threat to our business?

Do we have the telemetry (and capability) to develop detections for these techniques?

How do we respond to these alerts in "real-life" conditions (e.g., contextual awareness, time to detect etc)



Research



Map



Assess



Enhance



Validate

Which of these TTPs can be reliably tested and emulated in our environment?

Can we develop high-fidelity detection or mitigation strategies for these TTPs?



OUR REQUIREMENTS

WHAT WE WANTED FROM A PLATFORM

To help fulfil our organisations' requirement to be threat-intelligence led, we wanted a platform that could help orchestrate teams across the security function. We needed:

Flexibility

- Framework / Kill Chain agnostic
- Could meet our current and future requirements

Standards Compliance

- STIX / TAXII compliant
- Easy to export data to re-use elsewhere

Detail Orientated

- Ability to capture rich detail, both from a Red and Blue team perspective

Encouraged Collaboration

- Encourage intra-business collaboration
- But also support sharing with peers and trust groups

Single Tool Across Security

- A tool for analysts *as well* as management
- One tool, with multiple use cases (not just for CTI)





Alert

The file format and extension of 'tables.xls' don't match. The file could be corrupted or unsafe. Unless you trust its source, don't open it. Do you want to open it anyway?

Yes

No

TOOL REVIEWS

WHY WE PICKED VECTR

	Benefits	Considerations
Excel <i>Unsuitable</i>	<ul style="list-style-type: none"> ▪ No additional licensing required ▪ Can theoretically be built and customised to your specific use case 	<ul style="list-style-type: none"> ▪ Not optimised for multiple users ▪ Significant development time ▪ Excel not optimised for this task
Custom Tooling <i>Unsuitable</i>	<ul style="list-style-type: none"> ▪ Can be customised to meet all your development and productivity needs ▪ Would be fully compliant with all your business / security requirements 	<ul style="list-style-type: none"> ▪ Cost / time for development ▪ Would require ongoing development, to maintain alignment with changes to the Mitre framework
Unfetter <i>Unsuitable</i>	<ul style="list-style-type: none"> ▪ Free for all uses, including Enterprise ▪ Tool developed by the NSA, aiming to provide actor-centric security reviews ▪ STIX compliant 	<ul style="list-style-type: none"> ▪ Development ceased in 2018, and so Mitre alignment off-kilter ▪ Tool unstable and not very performant ▪ Tool not as extensive as VECTR
VECTR <i>Ideal</i>	<ul style="list-style-type: none"> ▪ Free for all uses, including Enterprise ▪ Kill Chain / framework agnostic, but fully supports Mitre Enterprise ▪ Actively maintained ▪ STIX/TAXII compliant ▪ Potential to automate testing in future ▪ Facilitates collaboration between teams 	<ul style="list-style-type: none"> ▪ Not designed initially to be intel-led ▪ Tool development driven by tool developers, with reduced influence to prioritise Enterprise features (but developers very receptive to feedback) ▪ Self-hosted, technology stack may not be compatible with internal standards

VECTR

CAMPAIGN AND ASSESSMENT TRACKER

VECTR is a platform designed to facilitate security teams through comprehensive threat simulation assessments. Attacks can be documented to gauge the effectiveness of defensive tools to help strengthen an organisations' security posture, and improve detection capabilities through historical performance tracking.

Common campaigns and use cases include:

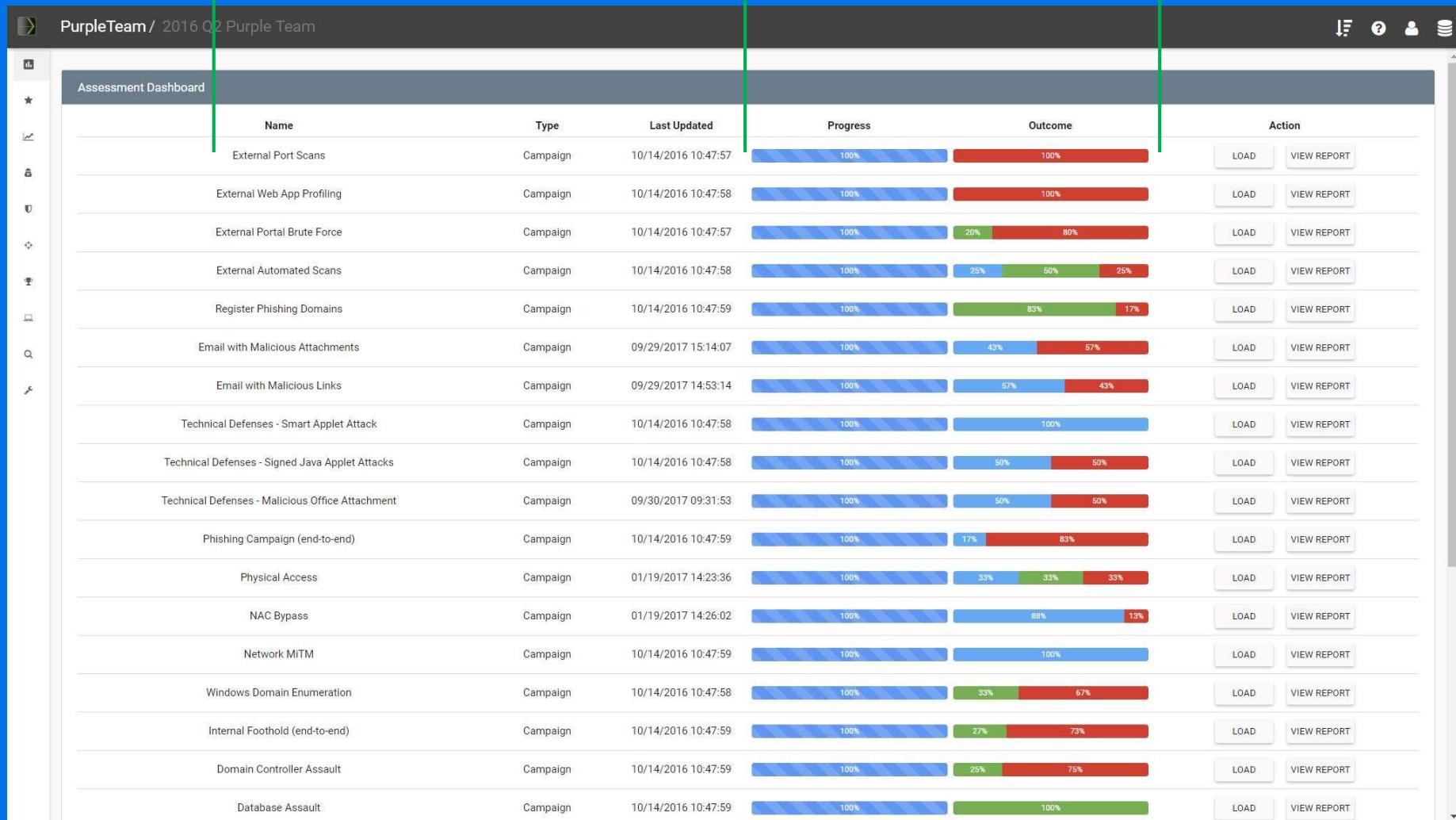
- Account abuse
- Spear phishing technical defences
- Malware detection and response
- Lateral movement and protected resources breach
- C2 and data exfiltration

- Ability to map prior attack methodologies in a consistent manner
- Measure progress across phases, campaign assessments, and outcomes
- Centralises Red Team and Blue Team techniques, allowing for control recommendations/tuning
- Ability to add custom test cases and target assets
- Produce summary and detailed reporting for campaign outcomes
- Provide historical trending of campaign exercises
- Rich management information; one tool for analysts and leaders

Each known cyber attack or attack type is loaded as a campaign

As TTPs are mapped and tested, the progress is updated

As a capability assessment is completed, the Outcome is updated



Swim lanes show an end-to-end view of an attack

Test Cases are specific implementations of a technique

Timeline and Outcome show the result of validation tests

SANS_DEMO / Adversary Emulation 2020 / APT19

APT19: Escalation Path

Timeline

- 07/01/2020 09:44:49 APT19 - Standard Application Layer Protocol - Cobalt Strike - Empire : outcome changed to Detected
- 07/01/2020 09:44:47 APT19 - Standard Application Layer Protocol - Cobalt Strike - Empire : status changed to Completed
- 07/01/2020 09:44:46 APT19 - Standard Application Layer Protocol - Cobalt Strike - Empire : status changed to InProgress
- 07/01/2020 09:44:36 APT19 - Drive-by Compromise : outcome changed to Blocked
- 07/01/2020 09:44:35 APT19 - Drive-by Compromise : status changed to Completed
- 07/01/2020 09:44:34 APT19 - Drive-by Compromise : status changed to InProgress

Test Cases

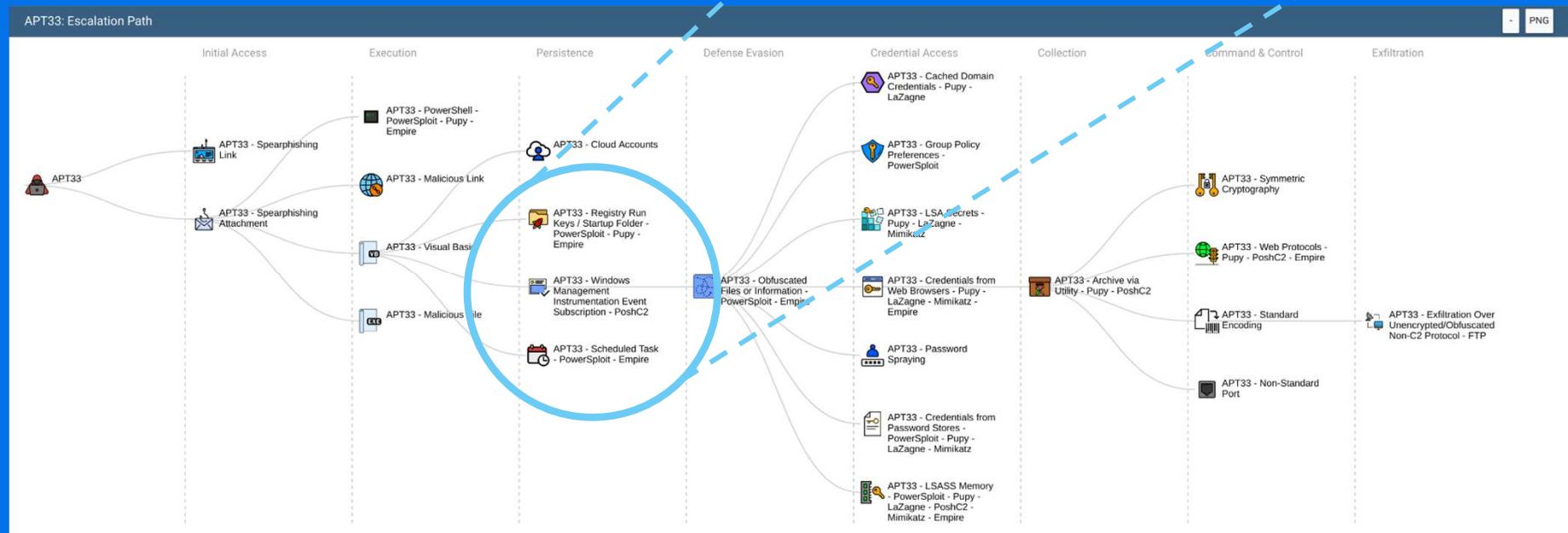
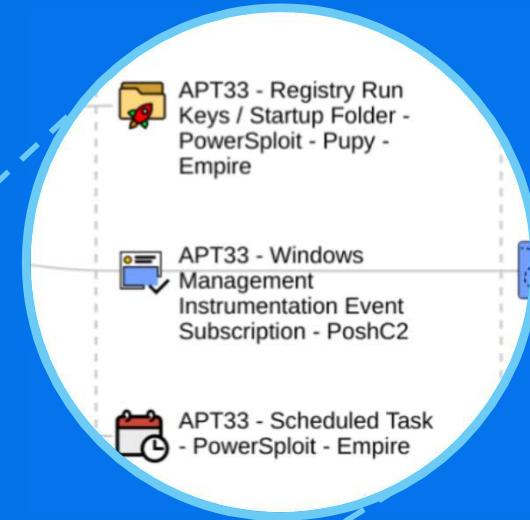
Phase	Technique	Test Case	Status	Outcome	Tags	Action
All	System Information Discovery	APT19 - System Information Discovery - Empire	Completed	Not Detected	High Priority	
Persistence	Registry Run Keys / Startup Folder	APT19 - Registry Run Keys / Startup Folder - Empire	Completed	Blocked		
Defense Evasion	DLL Side-Loading	APT19 - DLL Side-Loading	Completed	Not Detected	Medium Priority	
Execution	Regsvr32	APT19 - Regsvr32	Completed	Detected		
Initial Access	Drive-by Compromise	APT19 - Drive-by Compromise	Completed	Blocked		
Command & Control	Standard Application Layer Protocol	APT19 - Standard Application Layer Protocol - Cobalt Strike - Empire	Completed	Detected		

VECTR

ESCALATION PATH

A collection of Test Cases (TTPs) are used to illustrate an “Escalation Path”; which demonstrates the attacker’s movement across your preferred Kill Chain.

This is a simple, yet powerful way of summarising the adversary’s behaviour.



Red Team view shows specific offensive technique being tested

Edit Extract Logonpasswords via Dumper Test Case

Status: Completed

Attack Start

07/01/2020 09:54:20
status changed to InProgress

Attack Stop

07/01/2020 09:54:21
status changed to Completed

Source IPs

Linux VM

Red Team Details

Name: Extract Logonpasswords via Dumper

Description: Use dumper to extract credentials from LSASS process memory

Technique: Credential Dumping **Phase:** Credential Access

Operator Guidance: beacon>
dumper

References:

Attacker Tools

Dumper
Cobalt Strike

Target Assets

Target Laptop

Blue Team view shows specific defensive technique deployed

Blue Team Details

Outcome: TBD Blocked Detected NotDetected

Detecting Blue Tool(s):

EDR platform:
Was an alert triggered?
 Yes TBD No

Outcome Notes:
Ran dumper on target workstation, successfully blocked by EDR/NGAV agent and alerted via SIEM.

Tags:
High Priority **RE-TEST**

Rules

Detection

1) Suspicious process execution is detected by EDR or other endpoint security tool, or alerted in SIEM based on Windows or sysmon event IDs

Prevention

1) Suspicious process execution is blocked by EDR or other endpoint security tool

Detection Time

07/01/2020 09:55:48
outcome changed to Blocked

Expected

Detection Layers

SIEM
EDR
Endpoint Protection

Cancel

Save

Next

RED TEAM VIEW

ON THE OFFENSIVE

SAMPLE DATA

The screenshot displays the Red Team View application interface. On the left, there are four log cards: 'Status: Completed' (with icons for play, pause, stop, and up), 'Attack Start' (status 07/01/2020 09:54:20, changed to InProgress), 'Attack Stop' (status 07/01/2020 09:54:21, changed to Completed), and 'Source IPs' (Linux VM). The main area shows 'Red Team Details' for an operation named 'Extract Logonpasswords via Dumpert'. It includes sections for Name, Description, Technique (Credential Dumping), Phase (Credential Access), Operator Guidance (beacon> dumpert), References (+), and Attacker Tools (Dumpert, Cobalt Strike). Target Assets are listed as 'Target Laptop'. A red bar at the bottom indicates an active session.

- TTP intent and description
- Map to Mitre (or your preferred framework or Kill Chain)
- Capture rich metadata
- Set TTP icon
- Add references
- Map to existing offensive toolkits
- Specify target/scope
- And more!

TIP

Consider adopting the Atomic Red Team YAML specification

BLUE TEAM VIEW

CAPTURE THE DEFENCE

SAMPLE DATA

- Capture high level (vendor-agnostic) control
- TTP outcome
- Specific control responsible for detection or mitigation
- Add notes for defensive teams, including detection / prevention notes and corresponding evidence
- Map TTP directly to rules
- Tags to assist with workflow
- And more!

TIP

Consider adopting the SIGMA specification

The screenshot displays the Blue Team View interface, which is a digital dashboard for managing threat intelligence. It includes sections for 'Blue Team Details', 'Detection Time', 'Expected Detection Layers', and 'Detection'.

Blue Team Details:

- Outcome:** Blocked (checked), TBD, Detected, NotDetected.
- Detecting Blue Tool(s):** EDR platform.
- Was an alert triggered?** Yes (checked), TBD, No.
- Outcome Notes:** Ran dumpert on target workstation, successfully blocked by EDR/NGAV agent and alerted via SIEM.
- Tags:** High Priority, RE-TEST.
- Rules:** A section for defining detection rules.

Detection Time: 07/01/2020 09:55:48, outcome changed to Blocked.

Expected Detection Layers: SIEM, EDR, Endpoint Protection.

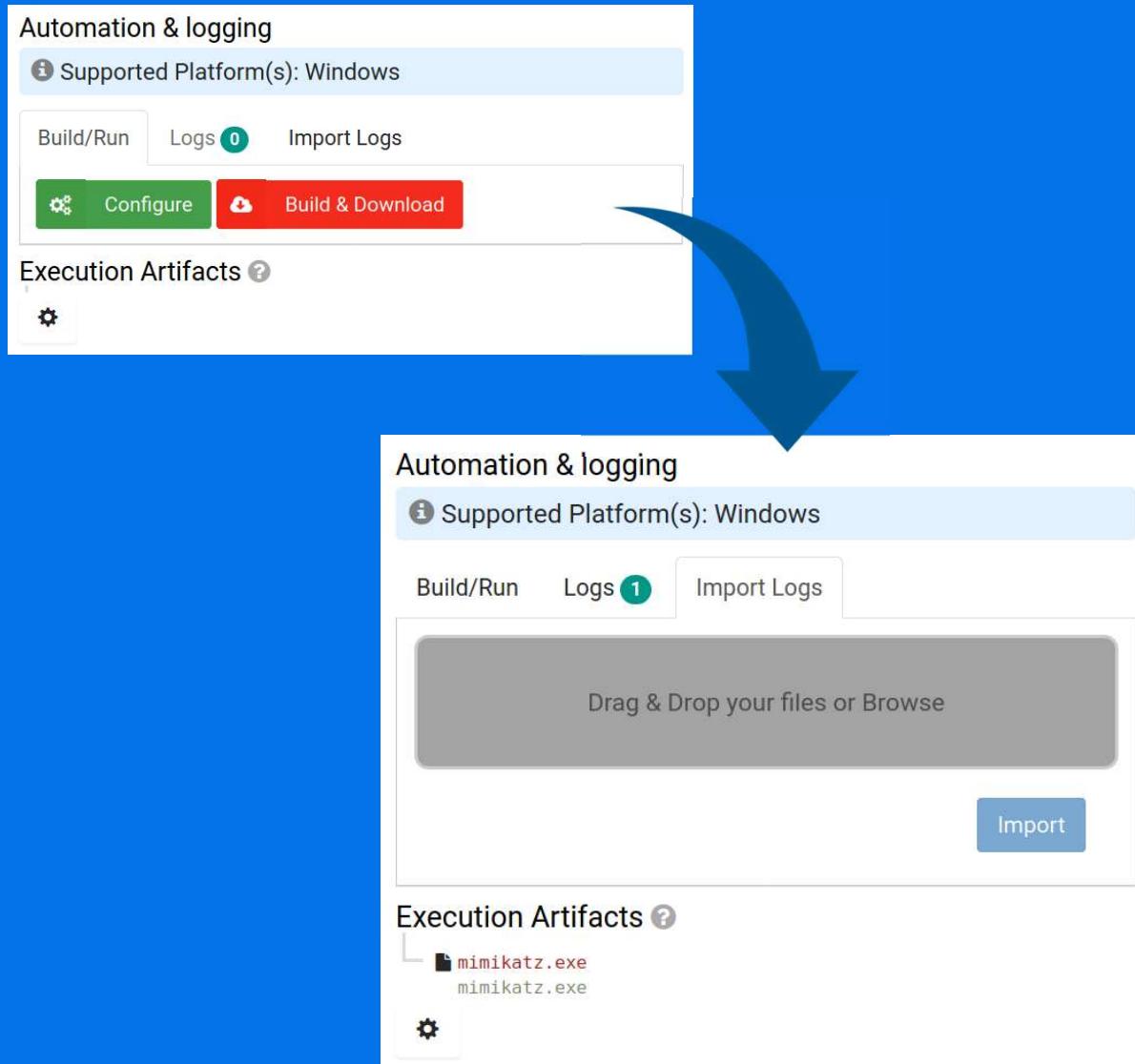
Detection:

- 1) Suspicious process execution is detected by EDR or other endpoint security tool, or alerted in SIEM based on Windows or sysmon event IDs.

TTP RUNTIMES

ATOMIC TEST BINARY GENERATION

NEW!



VECTR allows the production of Windows PE binaries that can be used to automate individual test cases or even entire campaigns.

- Supports cmd, PowerShell, and Inline PowerShell
- Allows supporting toolkits (“Execution Artefacts”) that can be dropped at runtime
- Can additionally clean-up after tests are executed
- Generates detailed logs which can be imported back into VECTR

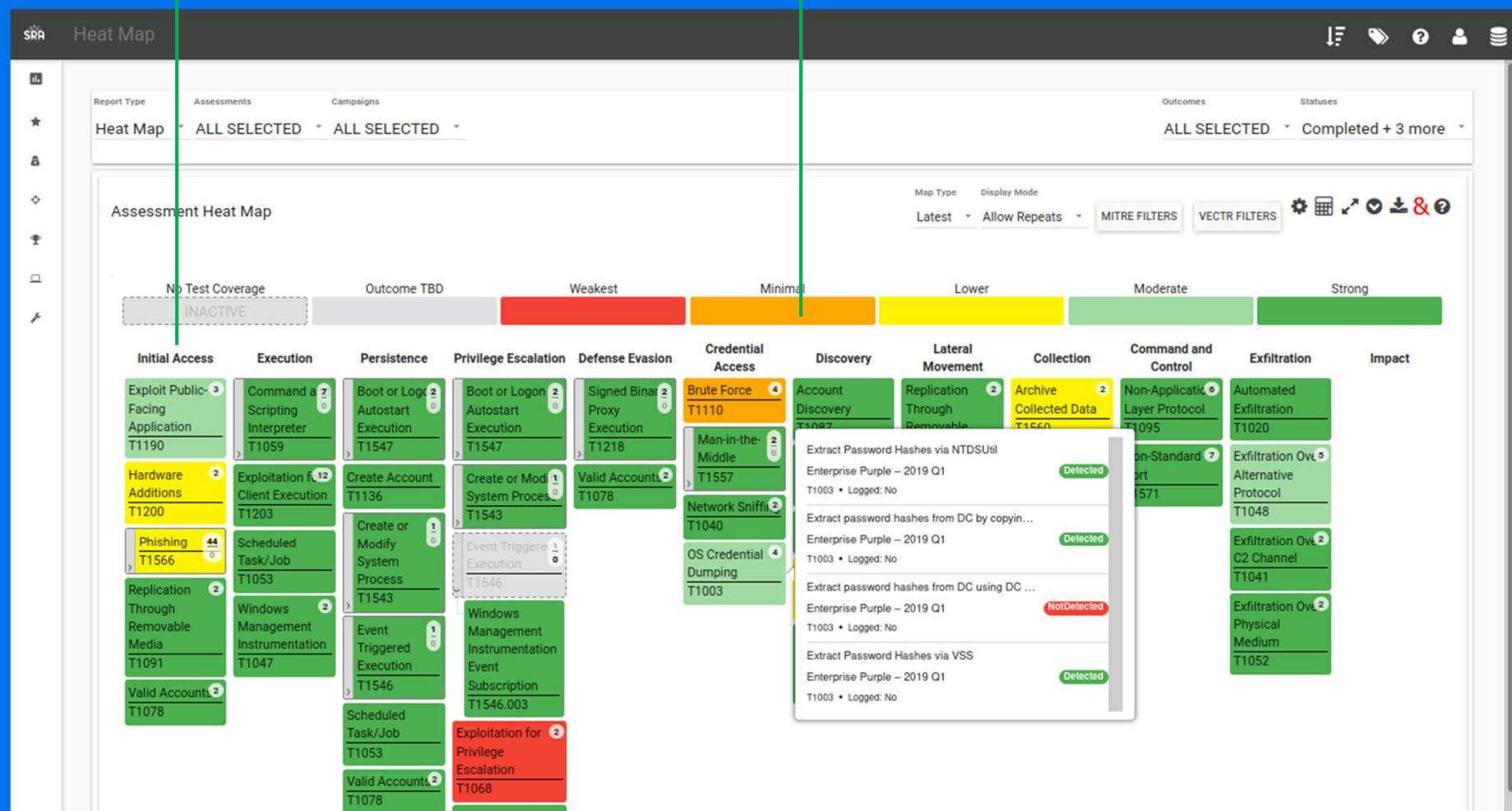
HEAT MAP

CONTROL EFFICACY HEATMAP VIEW

SAMPLE DATA

Heatmap view shows concentration of attacker TTPs grouped by tactic

Heatmap shows where controls are strongest, and opportunities for improvement



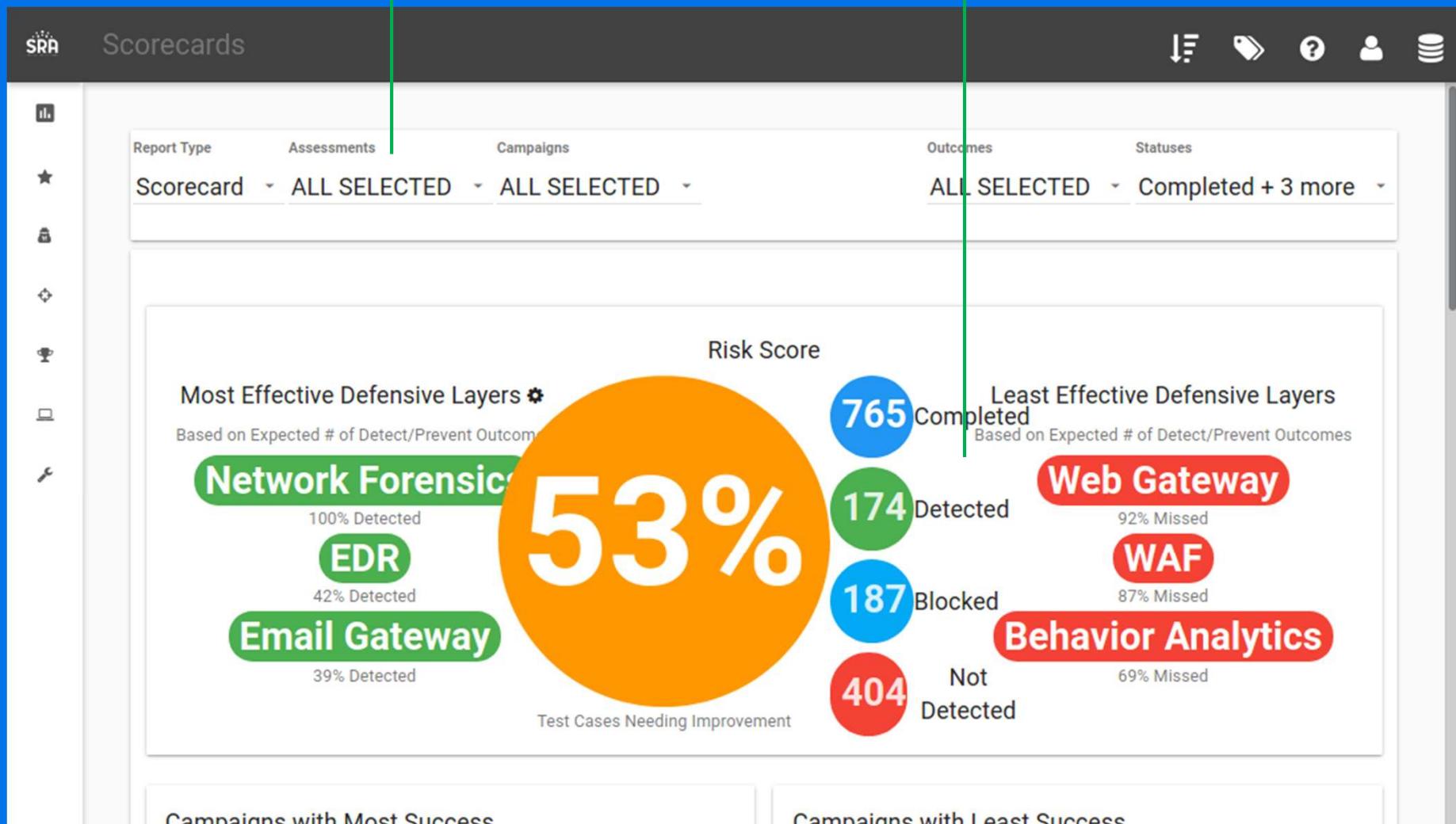
MANAGEMENT INFORMATION

SAMPLE DATA

CAMPAIGN ASSESSMENT DASHBOARD

Get a holistic view across all your tests, or specific campaigns

Campaign summary shows what you're good at, and what requires further development



TOOLSET SUMMARY

CONTROL EFFICACY REPORTING

SAMPLE DATA

Quickly see which specific controls are effective

Also see high-level, vendor-agnostic views of control posture



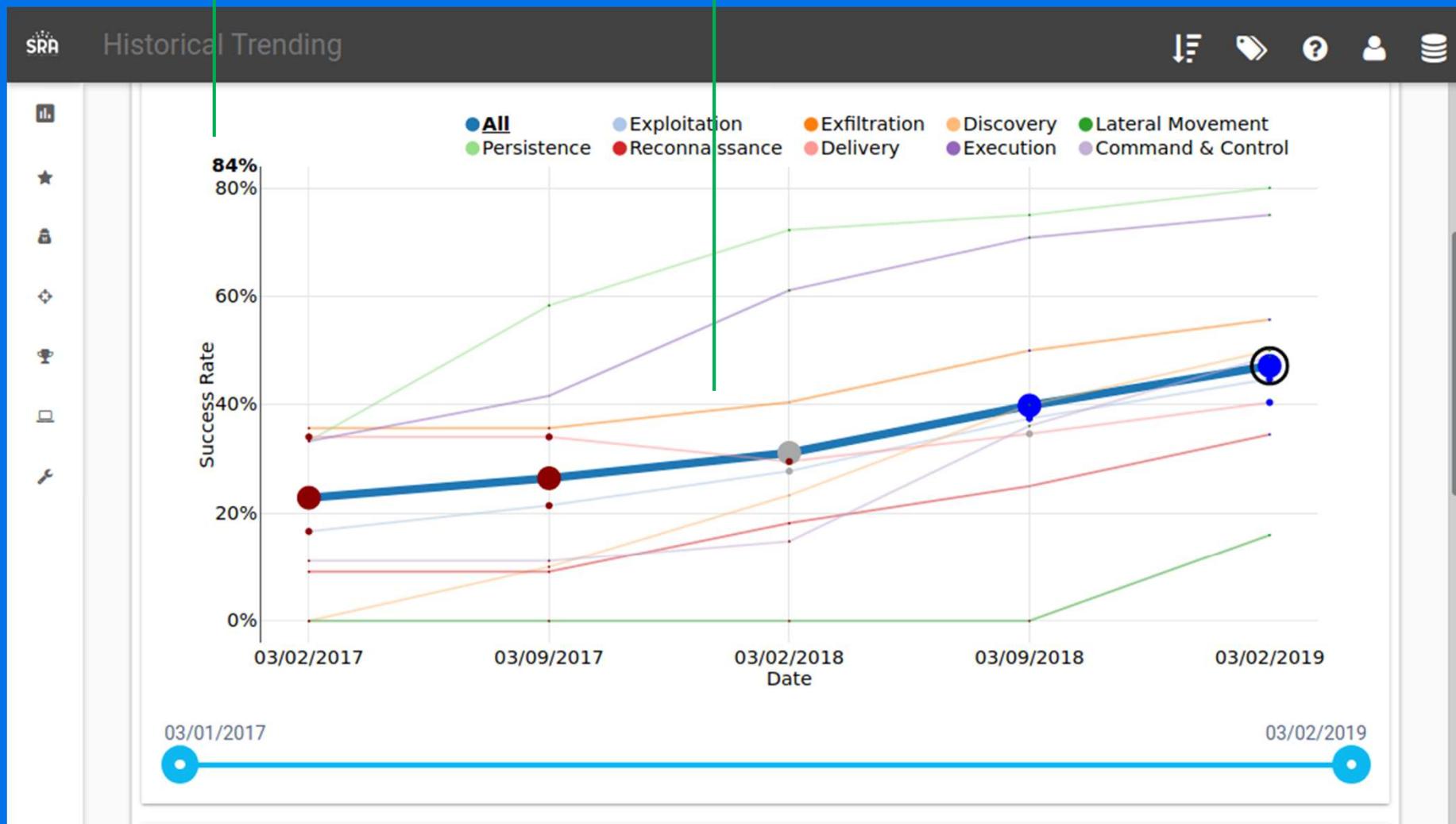
PROGRESS REPORTING

SAMPLE DATA

HISTORIC TRENDING VIEW

Over time,
dashboards provide
holistic view of
improvements

Tactic view shows
control efficacy by
Kill Chain phase



IMPORT

SUPPORTS YAML, JSON AND DIRECT IMPORT VIA TAXII SERVER

Supports importing directly from a STIX / TAXII server

Or manually, via YAML or JSON files

The screenshot shows the 'Import Data' interface. On the left is a vertical toolbar with icons for Home, Favorites, Collections, Recent, and Tools. The main area has a dark header bar with the SRA logo and 'Import Data' text, along with standard file operations like Save, Print, Help, User, and Settings.

The interface is divided into two main sections by vertical green lines:

- TAXII SERVER Section:** Contains a 'TAXII SERVER' button, a dropdown menu showing 'No Data', and a 'Edit TAXII Server Detail' button.
- JSON FILE Section:** Contains a 'JSON FILE' button, a description 'Alternative import method: VECTR data JSON file.', and a large grey area with the placeholder text 'Drag & Drop your files or Browse'.

A yellow 'OR' button is positioned between the two sections.

IMPORT

ATOMIC RED TEAM

Flexibility to import
one, some, or all
intrusion sets

The screenshot shows the SRA (Security Research Assistant) interface with a dark header bar containing icons for download, edit, help, user, and settings. On the left is a vertical sidebar with icons for Home, Star, Lock, Diamond, Trophy, and a wrench. The main content area has a title "Import Atomic Red" and instructions about importing from GitHub. It shows a summary of selected items: 0 Assessment Group Templates, 0 Campaigns, and 0 Total Test Cases Selected. Below this is a navigation bar with buttons for First, Previous, 1 (highlighted), Next, and Last. A list of campaigns is displayed in a scrollable table:

Campaign	Total Test Cases
Campaign: Collection	28
Campaign: Command & Control	32
Campaign: Credential Access	50
Campaign: Defense Evasion	211
Campaign: Discovery	102
Campaign: Execution	45

IMPORT

MITRE CTI BUNDLE

Flexibility to import
one, some, or all
intrusion sets

The screenshot shows the VECTR application interface with a dark header bar containing the SRA logo and various icons for file operations, search, and help.

Import STIX2 Data

Select Data from STIX2 Collection to be imported and merged with VECTR Data.
Top level items will be campaigns in VECTR, under each is a list of test cases and the STIX objects that comprise them.

Buttons: SELECT ALL, DESELECT ALL, Submit

Status: 0 Assessment Group Templates, 0 Campaigns, 0 Total Test Cases Selected.

Pagination: First, Previous, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, Next, Last

List of Campaigns:

- List of All Campaigns → 447 Total Campaigns. 5687 Total Test Cases.
- Campaign: 3PARA RAT → 4 Total Test Cases.
- Campaign: 4H RAT → 6 Total Test Cases.
- Campaign: ABK → 7 Total Test Cases.
- Campaign: ADVSTORESHELL → 24 Total Test Cases.
- Campaign: APT-C-36 → 8 Total Test Cases.
- Campaign: APT1 → 16 Total Test Cases.
- Campaign: APT12 → 5 Total Test Cases.

COLLABORATE

ACCELERATE ANALYSIS WITH PEERS

Export full intrusion campaigns to share with peers

The screenshot shows the GoldStandard Admin Assessment Configuration interface. On the left, the 'Manage Campaigns' panel lists two campaigns: 'SRA' and 'BBSRAT'. The 'BBSRAT' row includes columns for Name (BBSRAT), Organization (MITRE), Import Date (01 Sep 2020), and Action (with icons for edit, export, and delete). A green vertical line points from the 'Action' column to the 'Export to JSON File' button in the bottom right corner of the same row. On the right, the 'BBSRAT Details' panel displays a table of techniques categorized by Phase, Technique, Variant, and Action. The phases listed are Persistence, Command & Control, Defense Evasion, and Discovery. The techniques include Windows Service, Web Protocols, Process Hollowing, Commonly Used Port, Registry Run Keys / Startup Folder, Symmetric Cryptography, Deobfuscate/Decode Files or Information, System Service Discovery, Process Discovery, and File Deletion. Each technique has an edit and export icon in its Action column.

Phase	Technique	Variant	Action
Persistence	Windows Service	BBSRAT - Windows Service	
Command & Control	Web Protocols	BBSRAT - Web Protocols	
Defense Evasion	Process Hollowing	BBSRAT - Process Hollowing	
Command & Control	Commonly Used Port	BBSRAT - Commonly Used Port	
Persistence	Registry Run Keys / Startup Folder	BBSRAT - Registry Run Keys / Startup Folder	
Command & Control	Symmetric Cryptography	BBSRAT - Symmetric Cryptography	
Defense Evasion	Deobfuscate/Decode Files or Information	BBSRAT - Deobfuscate/Decode Files or Information	
Discovery	System Service Discovery	BBSRAT - System Service Discovery	
Discovery	Process Discovery	BBSRAT - Process Discovery	
Defense Evasion	File Deletion	BBSRAT - File Deletion	

COLLABORATE

ACCELERATE ANALYSIS WITH PEERS

Supports importing directly from a STIX / TAXII server

Flexibility to import one, some, or all intrusion sets

The screenshot shows the VECTR web application's interface. At the top, there's a navigation bar with icons for file operations, user management, and settings. Below the header, a section titled "Import VECTR Data" contains instructions: "Data to be imported from file and merged with VECTR Template Data." A summary row indicates "1 Assessment Group Templates, 7 Campaigns, 162 Total Test Cases Selected." A "Submit" button is located at the top right of this section. The main content area lists seven campaigns, each with a count of test cases: CopyKittens (6), OilRig (APT34) (44), MuddyWater (31), Collection of Iranian TTPs from US-CERT AA20-006A (15), APT39 (18), Magic Hound (27), and APT33 (21). Each campaign entry has a right-pointing arrow icon. On the far left, there's a vertical sidebar with various icons.

EXPORTING CAMPAIGN TEMPLATES ONLY SHARES THE RED VIEW

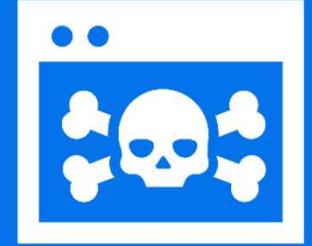
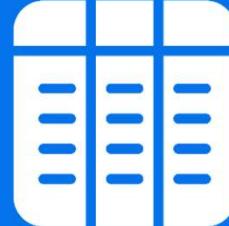
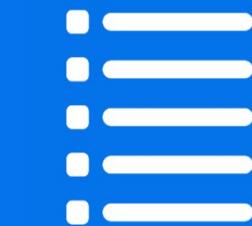
VECTR CONCEPTS

ADAPTING VECTR FOR ADVERSARIAL MODELLING

VECTR VISION



Database
For logical separation of assessments



Assessment
Typically after a period of time, such as Q1 2020

Campaign
Usually focussing around a specific TTP sprint

Test Case
A specific atomic test to be completed

OUR VISION



Team Use Case
One database per team within security



Threat Actor
To track specific threat actors of interest



Cyber Attack
Prominent cyber attack or tool used by the adversary

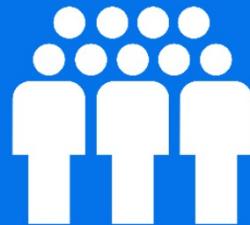


Specific Test
Specific way a tool was used by the adversary

VECTR CONCEPTS

PREPARING FOR ADVERSARY EMULATION

THREAT-LED



Team Use Case

One database per team within security

Threat Actor

To track specific threat actors of interest

Cyber Attack

Prominent cyber attack or tool used by the adversary

Specific Test

Specific way a tool was used by the adversary

THREAT RESEARCH



LAZARUS



BANK OF BANGLADESH



TTP 1

FAR EASTERN INTERNATIONAL BANK

TTP 2

TROY OPERATION

TTP 3

DARKSEOUL OPERATION

TTP 4

SONY PICTURES

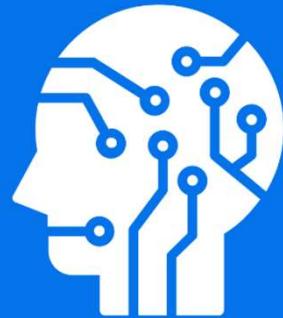
ETC

Not sure which threat actors or events are relevant? Read Chapter 7 “*Threat Intelligence for Risk Analysis*” by Recorded Future (free):

go.recordedfuture.com/book

VECTR-FY EVERYTHING

VECTR HERE, VECTR THERE, VECTR EVERYWHERE!



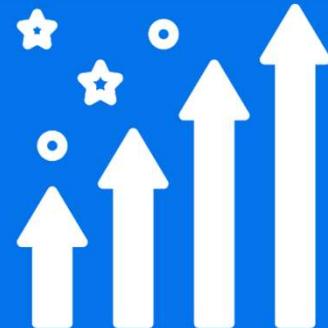
Threat Intelligence

Threat Intelligence teams can use VECTR to collate and organise known truths about a threat actor and their TTPs



Internal Incidents

Incident Responders can log novel incidents such as Phishing campaigns into VECTR, and use its powerful reporting views



Formal Engagements

Formal engagements, such as Pen Tests, can be loaded and actioned within VECTR

AND MUCH, MUCH MORE!

DEMO

LESSONS LEARNT

PREPARING FOR SUCCESS

1

Get Buy-In

For best results, get support from your teams as early as possible

2

Agree Responsibilities

Define clearly the roles of each SME team, to help industrialise outcomes

3

Create a Framework

Develop your own framework detailing research standards

“ The best preparation for tomorrow is doing your best today

— H. Jackson Brown Jr

FURTHER READING

AND HELPFUL RESOURCES

Purple Team Exercise Framework · SCYTHE

www.scythe.io/ptef



MITRE ATT&CK Defender — Fundamentals · Cybrary

www.cybrary.it/course/mitre-attack-defender-mad-attack-fundamentals

MITRE ATT&CK Defender — Cyber Threat Intelligence Certification · Cybrary

www.cybrary.it/course/mitre-attack-defender-mad-attack-for-cyber-threat-intelligence



MITRE ATT&CK — ATT&CK Evaluations · MITRE

attackevals.mitre-engenuity.org



TRAM · MITRE

github.com/center-for-threat-informed-defense/tram

Workbench · MITRE

ctid.mitre-engenuity.org/our-work/attack-workbench

CAPA · FireEye

github.com/mandiant/capa



QUESTIONS?

HERE TO HELP



Thank You for Participating

Tweet me at [@snkhan](https://twitter.com/@snkhan), or send a message via LinkedIn at linkedin.com/in/sajidnawazkhan.

Come Work for Us

www.sc.com/en/careers/jobseekers/

Getting Involved

SRA are currently developing a TTP Index for various industry sectors, including Finance. To get involved, and provide your input and expertise, please contact SRA at:

vectr@sra.io



PHOTOS FROM UNSPLASH

BREAK

After the break:
Hands-on workshop

HANDS-ON LAB



Access a copy of this presentation, complete with set-up guides, helper scripts and more at:

<https://github.com/ssnkhan/adversarial-threat-modelling>

INSTALLATION

PLEASE ACCEPT ALL DEFAULTS

```
sudo mkdir -p /opt/vectr  
cd /opt/vectr
```

TERMINAL

```
sudo wget  
https://github.com/SecurityRiskAdvisors/VECTR/releases/downl  
oad/ce-8.0.5/sra-vectr-runtime-8.0.5-ce.zip -P /opt/vectr  
sudo unzip sra-vectr-runtime-8.0.5-ce.zip
```

```
sudo nano .env          // Can be left as they are  
sudo nano /etc/hosts    // Add sravectr.internal  
docker-compose up -d     // May take a few minutes
```

TIP

For demonstration purposes, please use default configuration options.
Installation can take some time, so please start the process now

LAUNCHING VECTR

HELPER SCRIPTS

```
# Launch Vectr
cd /opt/vectr
sudo docker-compose up -d
sleep 30
firefox "https://sravectr.internal:8081/sra-purpletools-
webui/app/#"
```

TERMINAL

```
# Shutdown Vectr
cd /opt/vectr
sudo docker-compose down
```

TIP

Save these as `start_vectr.sh` and `shutdown_vectr.sh` in your home folder to quickly launch and safely shutdown your VECTR instance. Remember to `chmod +x`

SET UP: UNDERSTANDING SCOPE

LOCAL VS GLOBAL SCOPE

Configuration of offensive and defensive tooling (Vendor & Tools) as well as specific controls (Defensive Layers) can be set either locally for the current database, or globally; where they become available across all databases.

- **Local Scope** – Use this when you do not wish to persist customisations (including Test Cases) across other databases (e.g., where each database might represent a specific client)
- **Global Scope** – Use this if you wish to make your changes available across all your databases. This is best if your VECTR instance will be used entirely by your organisation

Local Scope

Global Scope

The screenshot shows the VECTR software interface. On the left is a navigation sidebar with the following items:

- Assessments
- Reporting
- Vendor & Tools
- Defensive Layers
- Target Assets
- Source IPs
- Administration
 - Group Templates
 - Campaign Templates
 - Test Cases
 - Vendor & Tools
 - Defensive Layers
 - Phases
 - Organizations
 - Kill Chains
 - Tagging
 - Detection Rules
 - Import Data
 - User Management

Below the sidebar is a table titled "Assessments" with the following data:

Name	Create Date
Enterprise Purple – 2017 Q1	01/03/2017
Enterprise Purple – 2017 Q3	08/03/2017
Enterprise Purple – 2018 Q1	01/03/2018
Enterprise Purple – 2018 Q3	08/03/2018
Enterprise Purple – 2019 Q1	01/03/2019

At the bottom right is the SRA logo: SECURITY RISK ADVISORS.

SET UP: ORGANISATIONS

CONFIGURING VECTR

Organisations allow you to capture and attribute the source of research or analysis within VECTR. It is sensible to create a separate organisation for any key contributor, such as:

- Teams within your organisation (such as Threat Intelligence, your SOC or Red Teams)
- Specific Trust Groups
- Vendors, where analysis is made available in STIX / TAXII format

TIP

If a business area has their own database, they should have their own organisation too

ADMINISTRATION > ORGANIZATIONS

New Organization

Name:	<input type="text"/>
Description:	<input type="text"/>
Abbreviation:	<input type="text"/>
Url:	<input type="text"/>
Members:	<input type="button" value="+"/>

SET UP: DATABASES

CONFIGURING VECTR

In VECTR, Session Databases are designed as a means of logically separating a collection of work or research.

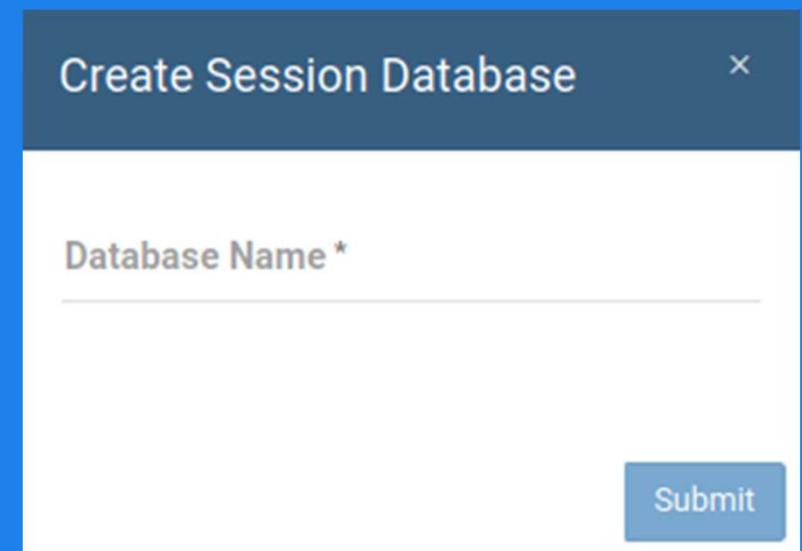
For instance, you may wish to create individual databases for:

- Threat intelligence led research
- Internal security Incidents
- Formal Pen Test findings
- Red Team Wiki
- Trust Groups / Collaboration

TIP

When considering a new database, think of the reporting implications

DB MENU > SELECT SESSION DATABASE



SET UP: PHASES

CONFIGURING VECTR

In VECTR, Phases are the term used to organise and configure specific frameworks that you may wish to use. Your chosen framework will then be accessible when capturing Test Cases, and for illustrating the Escalation Path. Good candidates include:

- Mitre ATT&CK
- Unified Kill Chain
- Lockheed Martin Kill Chain
- Your bespoke Kill Chain

TIP

The order of Phases determines the way in which the Escalation Path is drawn

ADMINISTRATION > PHASES

Mitre ATT&CK

INITIAL ACCESS EXECUTION PERSISTENCE
PRIVILEGE ESCALATION DEFENSE EVASION
CREDENTIAL ACCESS DISCOVERY
LATERAL MOVEMENT COLLECTION
COMMAND AND CONTROL EXFILTRATION IMPACT

Lockheed Martin Kill Chain

RECONNAISSANCE WEAPONISATION DELIVERY
EXPLOITATION INSTALLATION
COMMAND AND CONTROL ACTIONS ON OBJECTIVES

SET UP: TAGS

CONFIGURING VECTR

Tags are a powerful way of orchestrating actions within VECTR, and can serve as a helpful prompt to other teams within your organisation. For instance, you can use Tags to:

- Set the status of a piece of analysis
- Identify teams responsible for some output or analysis
- Set priorities for specific Test Cases
- Capture other internal metadata unique to your organisation or workflows

TIP

Consider including Tags as part of your workflow standards documents



Suggestions

QUEUED FOR ANALYSIS ANALYSING COMPLETE
ARCHIVED

QUEUED FOR ANALYSIS ANALYSING ENHANCING
CONTROL REVIEW VALIDATING COMPLETE

CTI SIEM TEAM FORENSICS MALWARE
ARCHITECTURE NETWORKS THREAT HUNTING

SET UP: VENDORS & TOOLS

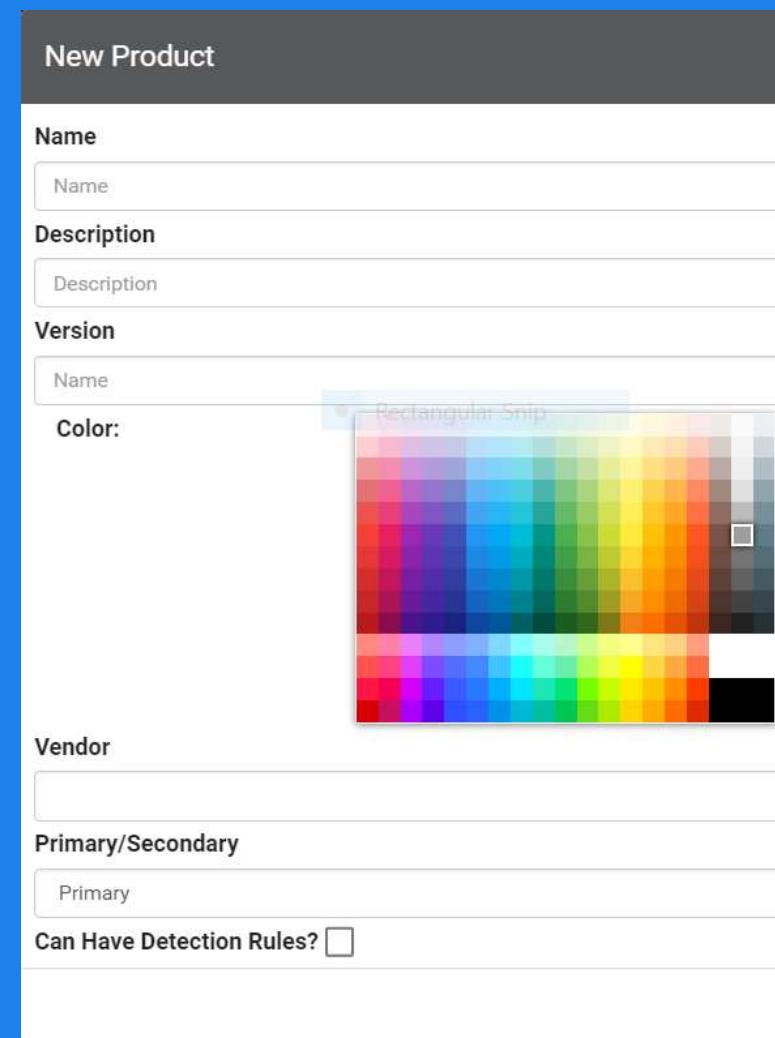
CONFIGURING VECTR

A lot of the value in using VECTR is being able to understand which specific controls are responsible for detecting and blocking specific techniques. Setting these correctly ensures your controls receive the appropriate kudos.

- **Defensive Layers** – These should be high-level, vendor agnostic controls (e.g., Web Proxy)
- **Vendors & Tools** – These should represent the specific controls in your environment (e.g., FireEye EX)

TIP

Remember to set your Vendor tool appropriately under “Can Have Detection Rules”



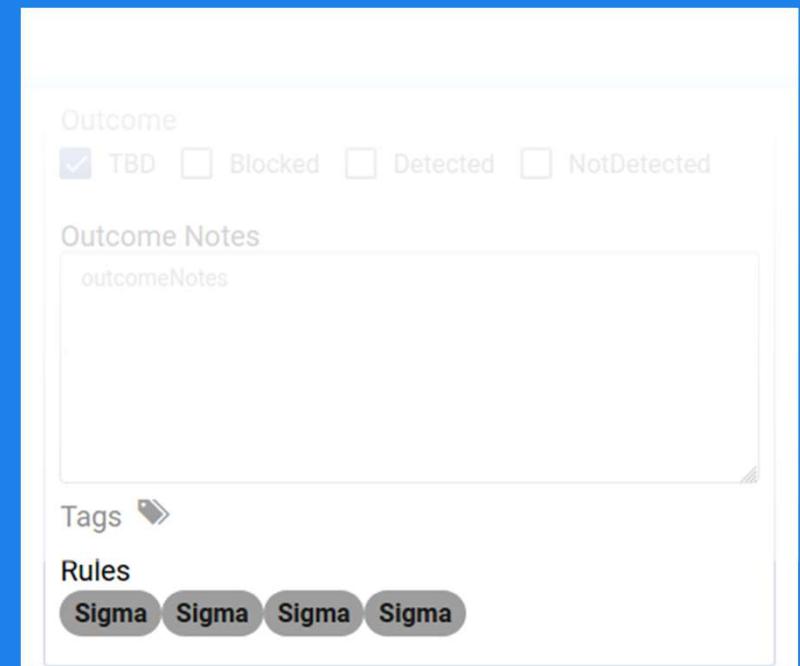
SET UP: DETECTION RULES

CONFIGURING VECTR

Detection rules allow signatures to be mapped to specific TTP Test Cases; to help continue developing a full view of the TTPs effect in your environment, and can support Threat Hunting initiatives.

- **Data Sources** – Reflect the various telemetry which underpins your ability to develop detections
- **Generic Sources** – Vendor agnostic, such as JA3, Sigma or YARA
- **Generic Rules** – The actual rules
- **Analysis Rules** – Vendor specific rules, such as Splunk, Tanium Signals
- **Behaviours** – Behaviours are the mechanism which link your rules to their corresponding TTPs

ADMINISTRATION > DETECTION RULES



The following video demonstrates the process:
youtu.be/Xt2JsbNnUCA

TIPS & TRICKS

GET THE MOST OUT OF VECTR

Actor Naming

- Hidden Cobra, Lazarus, Bluenoroff, Labyrinth Chollima or ...? Agree on a common naming taxonomy:

APT38 · Lazarus · Hidden Cobra

Campaign Naming

- Consider prefixing all campaigns with date serialisation to quickly sort chronologically:
YYYYMMDD Campaign:

20160204 Bank of Bangladesh

Abort FYI Use Cases

- To prevent polluting your management information with “FYI” only Test Cases, abort them in the Red Team view:

Assessment → Campaign → Test Case → 

Key-Value Pairs

- In both Red and Blue team views, establish standardised key-value pairs to capture data:

`md5:value sha1:value leadTester:staffID`

EXERCISES: IMPORT

PRACTICAL EXAMPLES TO GET YOU UP AND RUNNING

1

Mitre CTI Bundle

github.com/mitre/cti/blob/master/enterprise-attack/enterprise-attack.json

2

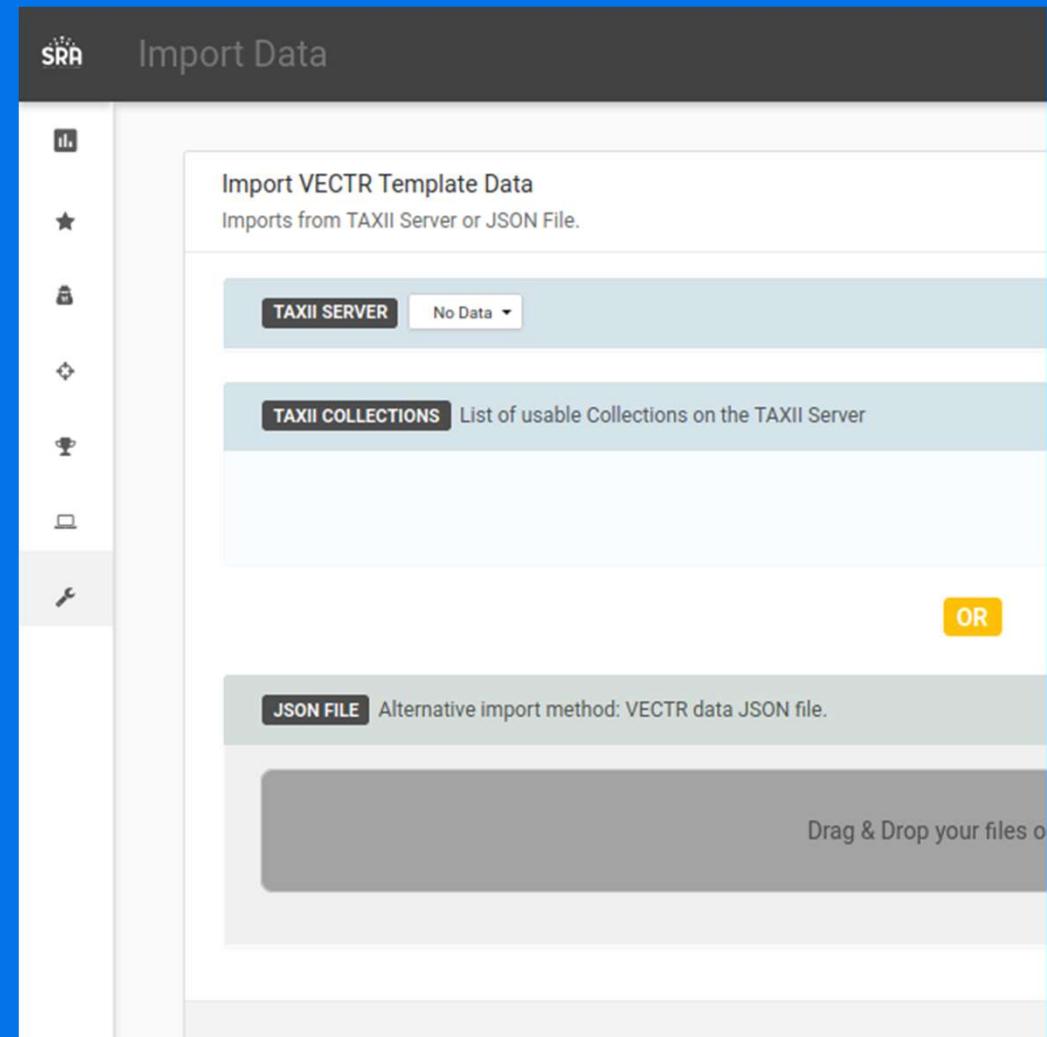
Atomic Red Team

github.com/redcanaryco/atomic-red-team/blob/master/atomics/indexes/index.yaml

3

SRA Iran Analysis

github.com/SecurityRiskAdvisors/VECTR/tree/master/cti



EXERCISES: THREAT LIBRARY

PRACTICAL EXAMPLES TO GET YOU UP AND RUNNING

The rest of the session will be used to complete a few exercises to help develop your confidence and familiarity with VECTR — pan-unit42.github.io/playbook_viewer/

The screenshot shows a web browser window titled "UNIT 42 PLAYBOOK VIEWER" with the URL "pan-unit42.github.io/playbook_viewer/?pb=sofacy". The interface includes a sidebar with filters for various threat groups like OILRIG, SOFACY, PICKAXE, PATCHWORK, DARKHYDRUS, REAPER, RANCOR, TICK, DRAGONOK, MENUPASS, EMISSARY PANDA, and MINDWALTERED. The main content area displays information about the Sofacy threat group, including its activity timeline from October 2018 to November 2018, and a detailed view of its campaigns, indicators, and attack patterns. It also shows a kill chain table for Lockheed Martin.

PLAYBOOK WALKTHROUGH
VIEW HOME
VIEW MAP
FILTER PLAYBOOKS
CLEAR FILTERS

OILRIG

SOFACY

PICKAXE

PATCHWORK

DARKHYDRUS

REAPER

RANCOR

TICK

DRAGONOK

MENUPASS

EMISSARY PANDA

MINDWALTERED

Created by Palo Alto Networks - Unit 42
Mitre Attack™ TTX 2.0

PLAYBOOK VIEWER

October 2018 to November 2018

October 2018 to October 2018

March 2018 to March 2018

February 2018 to February 2018

Sofacy (also known as Fancy Bear, APT 28, STRONTIUM, Pawn Storm) is a highly active actor with a Russian nexus. They have been active since the mid 2000s, and have been responsible for targeted intrusion campaigns against various industry vertical such as but not limited to Aerospace, Defense, Energy, Government and Media. Extensive observation and research of Sofacy's activities over time indicated a profile closely mirroring the strategic interests of the Russian government. More recently, this group has been attributed to the GRU, Russia's premier military intelligence service as reported by the US intelligence community within several declassified public documents.

Sofacy group continued their global attack campaigns between October and November. In this campaign, the Sofacy group appears to have relied heavily on filenames to lure victims into launching the weaponized documents, primarily targeting NATO-aligned nation states and former USSR states and delivering Zebrocy or Cannon.

Intrusion Set: Sofacy Campaigns: 4 Indicators: 51 Attack Patterns: 34

Industries: Regions: Malware Used: Cannon, Zebrocy

Select Kill Chain [Lockheed Martin]

Reconnaissance	Weaponization	Delivery	Exploitation	Installation	Command & Control	Actions on Objectives
		T1566.001: Spearphishing Attachment 27		T1047: Windows Management Instrumentation 1	T1071: Application Layer Protocol 7	T1113: Screen Capture 0
				T1070.006: Timestamp 1	T1104: Multi-Stage Channels 0	T1082: System Information Discovery 2
				T1112: Modify Registry 1	T1105: Ingress Tool Transfer 0	T1057: Process Discovery 2

here for
good™