

Beyond Indicators: Scalable Network Defense

Jason Mok – Initiative Lead

Will Burger – Initiative Lead

Keat Ly – Integration Engineer

Amar Paul – Integration Engineer



- **Why?**
- **Adversary Playbooks**
- **MITRE ATT&CK**
 - How can it be used to share behaviors
 - Detections
- **Live Attack + Respond Campaign Demonstration**
- **Lessons Learned**

Driving Motivations



- **Want to move away from indicators**
 - Short shelf life
 - Dead on arrival
- **Want to move “Left of the Boom”**
 - Share TTPs, specifically *TTorPs*
- **Want to stay machine consumable and therefore, automatable**

- **Lots of Indicators. Hashes, IPs/URLs, Domains**
 - Enriched
 - Checked by analyst (sometimes)
 - Acted on
- **Automation exists, but current approaches still yields “Whack a Mole” approach**
- **TTPs always related to as one thing, rather than “T , T , or P”**

TTPs and Instances

Playbook Element	Description	Enables
Tactics	Provides the What & Why	Capability Identification, Proactive Measures, Policy
Techniques	How (Tech Agnostic)	Capability Assessment, Policy, Defensive Measurement Design
Procedures	How (Tech Specific)	Workflow development, Detections, Tailoring Guidance for Enterprises
Instances	How (Examples)	Detections and Incident Response

Investigation



- Adversary Playbooks by Palo Alto's Unit 42
- Many different campaigns -> TTPs
- Maps to ATT&CK
- STIX Friendly

The screenshot displays the 'PLAYBOOK VIEWER' interface for the 'REAPER' playbook. On the left, a sidebar lists various playbooks, with 'REAPER' highlighted. The main content area provides a detailed description of the Reaper group, noting its focus on North Korean cyber espionage and its targets in South Korea, Japan, Vietnam, Nepal, Kuwait, and the Middle East. It also mentions the group's use of spear phishing, malware delivery, and compromise of strategic websites.

Below the description, a summary bar indicates: 'Intrusion Set: Reaper', 'Campaigns: 5', 'Indicators: 46 (Click For Overview)', and 'Attack Patterns: 28'. The interface then maps the playbook's steps to the MITRE ATT&CK framework, showing a sequence of tactics from Reconnaissance to Objective.

RECON	WEAPONIZATION	DELIVERY	EXPLOIT	INSTALL	COMMAND	OBJECTIVE
T1241: Determine strategic target	T1345: Create custom payloads	T1193: Spearphishing Attachment		T1102: Web Service	T1071: Standard Application Layer Protocol	T1041: Exfiltration Over Command and Control Channel
					T1102: Web Service	T1092: System Information Discovery

Investigation (Contd.)

- **MITRE's ATT&CK**

- **Comprehensive**
- **Separated by Tactics**
 - Lots of techniques
 - Expands into Procedures

- **Picked at least 1 technique out of each of all 11 tactics categories**

- **Influenced by Unit 42's most common techniques**

ATT&CK Matrix for Enterprise

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control
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	BITS Jobs	Bash History	Application Window Discovery	Application Deployment Software	Automated Collection	Data Compressed	Communication Through Removable Media
Hardware Additions	Command-Line Interface	Account Manipulation	AppCert DLLs	Binary Padding	Brute Force	Browser Bookmark Discovery	Distributed Component Object Model	Clipboard Data	Data Encrypted	Connection Proxy
Replication Through Removable Media	Compiled HTML File	AppCert DLLs	AppInit DLLs	Bypass User Account Control	Credential Dumping	File and Directory Discovery	Exploitation of Remote Services	Data Staged	Data Transfer Size Limits	Custom Command and Control Protocol
Spearphishing Attachment	Control Panel Items	AppInit DLLs	Application Shimming	CMSTP	Credentials in Files	Network Service Scanning	Logon Scripts	Data from Information Repositories	Exfiltration Over Alternative Protocol	Custom Cryptographic Protocol
Spearphishing Link	Dynamic Data Exchange	Application Shimming	Bypass User Account Control	Clear Command History	Credentials in Registry	Network Share Discovery	Pass the Hash	Data from Local System	Exfiltration Over Command and Control Channel	Data Encoding
Spearphishing via Service	Execution through API	Authentication Package	DLL Search Order Hijacking	Code Signing	Exploitation for Credential Access	Network Sniffing	Pass the Ticket	Data from Network Shared Drive	Exfiltration Over Other Network Medium	Data Obfuscation
Supply Chain Compromise	Execution through Module Load	BITS Jobs	Dylib Hijacking	Compiled HTML File	Forced Authentication	Password Policy Discovery	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Physical Medium	Domain Fronting
Trusted Relationship	Exploitation for Client Execution	Bootkit	Exploitation for Privilege Escalation	Component Firmware	Hooking	Peripheral Device Discovery	Remote File Copy	Email Collection	Scheduled Transfer	Fallback Channels
Valid Accounts	Graphical User Interface	Browser Extensions	Extra Window Memory Injection	Component Object Model Hijacking	Input Capture	Permission Groups Discovery	Remote Services	Input Capture		Multi-Stage Channels
	InstallUtil	Change Default File Association	File System Permissions Weakness	Control Panel Items	Input Prompt	Process Discovery	Replication Through Removable Media	Man in the Browser		Multi-hop Proxy
	LSASS Driver	Component Firmware	Hooking	DCShadow	Kerberoasting	Query Registry	SSH Hijacking	Screen Capture		Multiband Communication
	Launchctl	Component Object Model Hijacking	Image File Execution Options Injection	DLL Search Order Hijacking	Keychain	Remote System Discovery	Shared Webroot	Video Capture		Multilayer Encryption
	Local Job Scheduling	Create Account	Launch Daemon	DLL Side-Loading	LLMNR/NBTNS Poisoning	Security Software Discovery	Taint Shared Content			Port Knocking

ATT&CK Techniques Chosen



- **Spear-phishing attachment (Initial Access)**
- **Port Scan (Discovery)**
- **Standard application layer protocol (Command and Control)**
- **Registry Run Keys (Persistence)**
- **Scheduled Tasks (Persistence)**
- **Remote file copy (Lateral Movement/Command and Control)**
- **Exfiltration over Command and Control Channel (Exfiltration)**
- **Credentials in Files (Credential Access)**
- **Admin Shares (Lateral movement)**



Detections



- **Integration team wrote detections for ATT&CK techniques**
 - Get a gauge of the difficulty doing so
- **Able to use this experience to weight how important specific information is in sharing threat behavior**
- **Information exchange with Defense Point and APL ITSD**
- **MDR – “Detections as a Service”**



DEFENSE POINT
SECURITY

What to Share?



- **Adversary playbook**
 - Lacks certain details
 - Ingest options are not currently well-defined
- **The detection**
 - No “standard” way to express the process
 - Back to MDR
 - Alerts as a service

Branch: master | [playbook_viewer](#) / [playbook_json](#) / [darkhydrus.json](#) Find file Copy path

eiyuki Include updated CSS to match the new Unit 42 blog. Update the publish... 585add1 on Dec 18, 2018

2 contributors

2106 lines (2106 sloc) 103 KB Raw Blame History

```
1 {
2   "type": "bundle",
3   "id": "bundle--59afb48d-0f9c-434d-be6a-69515424b0c3",
4   "spec_version": "2.0",
5   "objects": [
6     {
7       "type": "report",
8       "id": "report--59afb48d-0f9c-434d-be6a-69515424b0c3",
9       "created": "2018-08-03T21:03:51.484Z",
10      "modified": "2018-08-03T21:03:51.484Z",
11      "name": "DarkHydrus",
12      "description": "DarkHydrus is a threat group targetting government agencies and educational institutions in",
13      "published": "2018-08-03T21:03:51.484Z",
14      "object_refs": [
15        "intrusion-set--e0edd713-cfcd-4252-859e-db12dbbde365",
16        "report--6320584e-3ef0-4a72-aaf8-0a49fa1d477c"
17      ],
18      "labels": [
19        "intrusion-set"
20      ]
21    }
22  ]
23 }
```

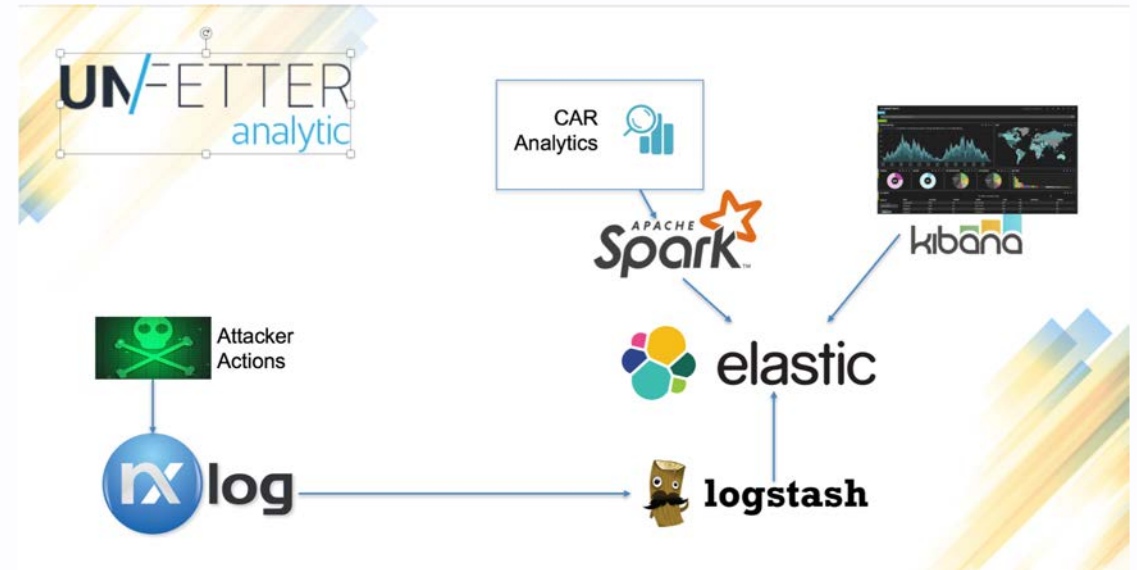
- Take alerts, investigate them, form correlations
- STIX 1.x on its way out
- STIX 2.x still has low adoption
 - Many developers waiting for STIX 2.1 release
- Tie together multiple Alerts
 - Format them -> share these

```
{
  "correlation":
  {
    "seconds_time_range_lt": 600,
    "relationships": [
      ["email", "user"],
      ["user", "host"],
      ["host", "dns"],
    ],
    "email": {
      "attachment": true,
      "poor_grammar": true,
    },
    "dns": {
      "num_requests_gt": 10,
      "byte_size_of_request_gt": 800,
      "type": "or"
    },
    "user": {
      "number_login_attempts_gt": 10,
      "number_target_hosts_gt": 1,
    },
    "host": {
      "percent_cpu_usage_gt": 80
    }
  }
}
```

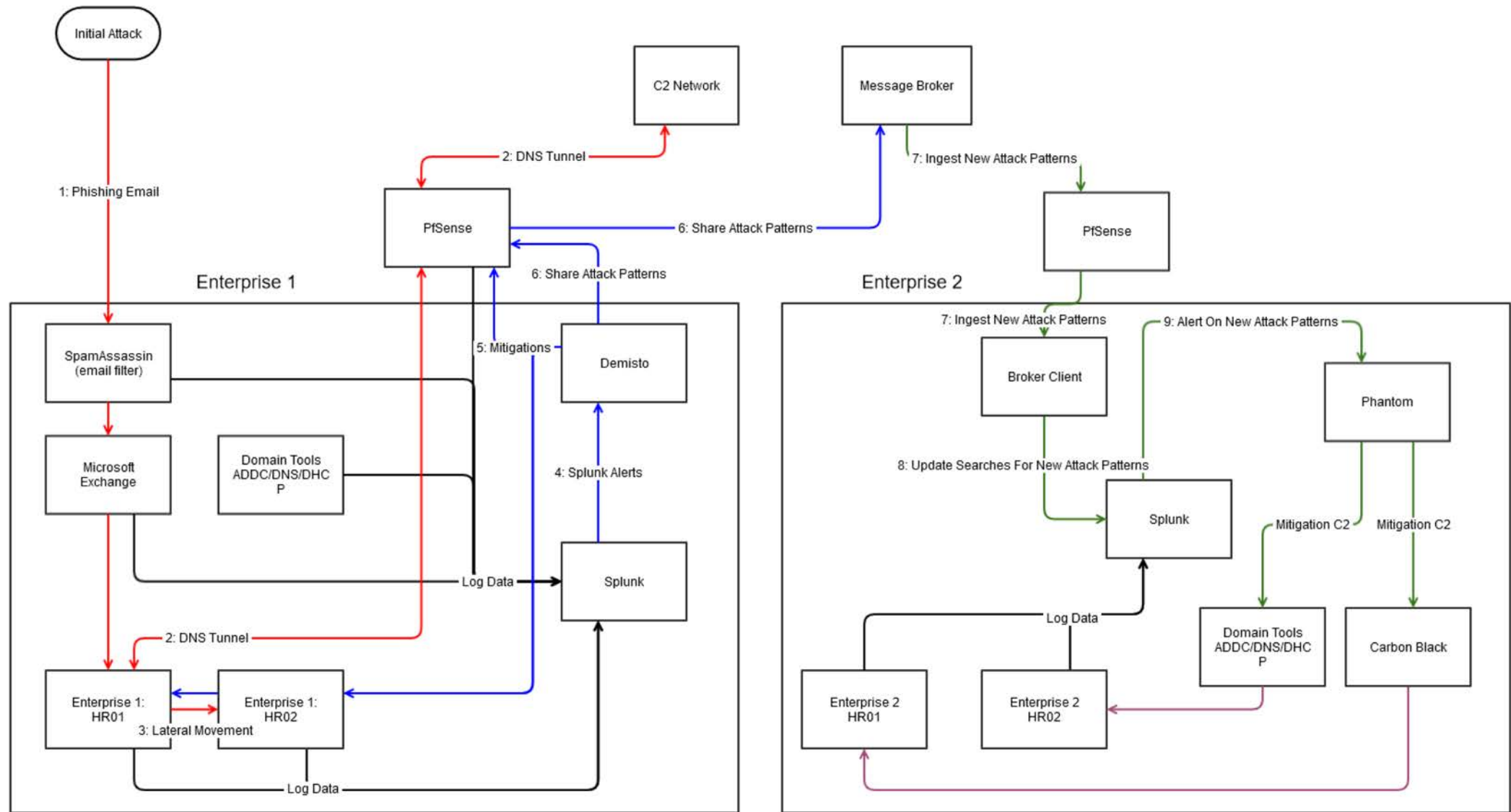
Building from Behaviors to TTPs

- **MITRE's Cyber Analytic Repository (CAR)**
- **Implemented in Unfetter currently**
- **Potentially the future of these behaviors is sharing analytics once they are developed**

MITRE Cyber Analytics Repository




Experiment Design



Experiment Technologies



Attacker	Enterprise 1	Enterprise 2	Broker
 	  	  	

Assumptions



- **Implicit Trust already established**
- **Vendor agnostic message fabric**
 - **To be replaced by standard transport mechanism**

Demo

Lessons Learned: Sharing



- **Need a standard for sharing behaviors**
 - STIX does not have “behavior” fields
 - One step closer to sharing an entire TTP
 - Can be used to build campaigns
- **Cognizant of differing organizational policy**
 - **Ex. Alerting on Rogue PowerShell**
 - Enterprise may give everyone admin access
 - **Ex. Testbed is monitored**

Lessons Learned: Implementation



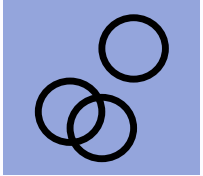
- **Splunk Alerts**
 - Want to trigger on incoming data
 - How to look in history for situational awareness
 - Safe from behavior in the future
- **API offers large number of fields for alerts**
 - Good: scripts have a lot of power
 - Bad: have to be extremely specific

Future Work



- **Modifying STIX 2.x to be able to properly encapsulate data**
- **OR need a new way to model behavior**
- **Engaging ISACs to share more actionable information**

The Future Ecosystem



Circles of Trust

Organizations are going to belong to multiple groups with different levels of trust. Some will have some relationship with another trust circle and some will be independent.

The Future Ecosystem



Information sharing and cyber defense automation share the same ecosystem



Shared information will directly feed risk decisions and associated automated processes.

Automated defenses will directly inform information sharing activities.

Questions?



Integrated Adaptive Cyber Defense is sponsored by the Department of Homeland Security and the National Security Agency in collaboration with The Johns Hopkins University Applied Physics Laboratory.

Our goal is to dramatically change the timeline and effectiveness of cyber defense via integration, automation, and information sharing.



<https://secwww.jhuapl.edu/iacd>



<https://www.linkedin.com/groups/8608114>



@IACD_automate



icd@jhuapl.edu