CYBERSEER

From IOC to TTP:

How Attack Chains Have Evolved

Session Agenda

CYBERSEER

- What is an IoC
- How are IoCs used
- IoCs applied to cyber kill chain
- What are TTPs
- How are TTPs used
- TTPs + Analytics
- TTPs applied to cyber kill chain
- Why TTPs are the future of detection and Threat Hunting

What is an IoC?

CYBERSEER

Indicators of Compromise (IOC) is an artifact observed on a network or in an operation system that with high confidence indicates a computer intrusion. (from Wikipedia)

- AV signatures
- Hashes
- Files Names
- IPs
- ULRs/Domains
- Behaviors

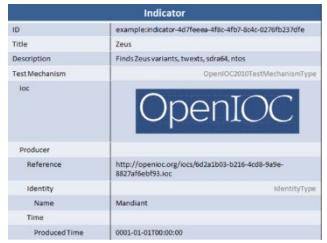
	A	B	C	D	E
1	INDICATOR_VALUE	TYPE	COMMENT	ROLE	ATTACK_PHA
2	efax[.]pfdregistry[.]net/eFax/37486[.]ZIP	URL		URL WATCHLIST	
3	private[.]directinvesting[.]com	FQDN		C2	C2
4	www[.]cderlearn[.]com	FQDN		C2	C2
5	46[.]4[.]193[.]146	IPV4ADDR		IP_WATCHLIST	
6	65[.]15[.]88[.]243	IPV4ADDR		IP_WATCHLIST	
7	185[.]104[.]11[.]154	IPV4ADDR		IP_WATCHLIST	
8	185[.]104[.]9[.]39	IPV4ADDR		IP_WATCHLIST	
9	8F154D23AC2071D7F179959AABA37AD5	MD5	FILENAME:DFDTS.DLL|FILE_SIZE:435712|SHA1:8CCAA941A	FILE HASH WATCHLIST	
10	AE7E3E531494B201FBF6021066DDD188	MD5	FILENAME:HRDG022184_certclint.dll |FILE_SIZE:434688|S	FILE HASH WATCHLIST	
11	7FCE89D5E3D59D8E849D55D604B70A6F	MD5		FILE HASH WATCHLIST	
12	81F1AF277010CB78755F08DFCC379CA6	MD5		FILE HASH WATCHLIST	
13	617BA99BE8A7D0771628344D209E9D8A	MD5		FILE HASH WATCHLIST	

*GRIZZLY STEPPE IOCS (911)

Evolution of IoCs & Birth of TTP's

Not much has changed

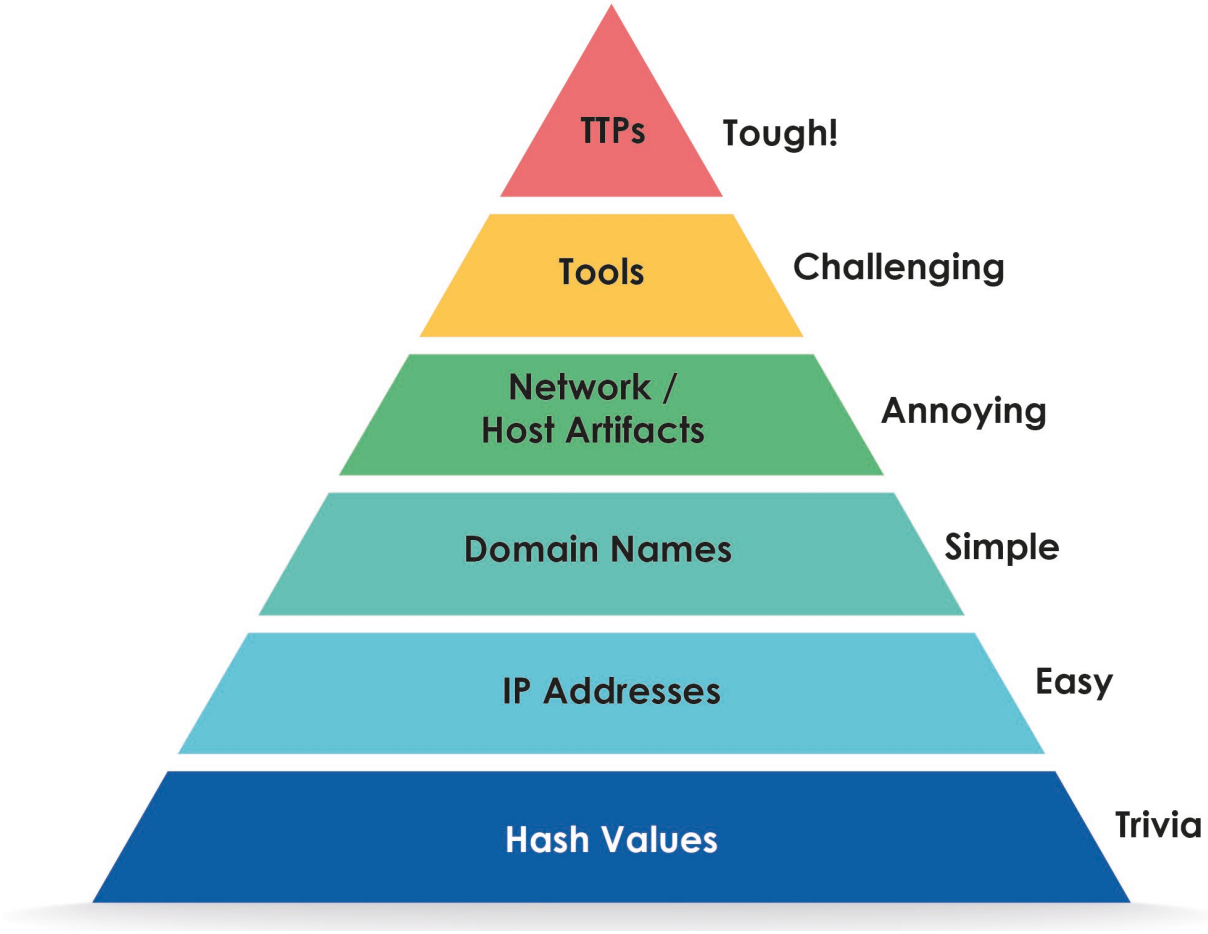
CYBERSEER



1985 1990 1995 2000 2005 2010 2015 2020

AV | Firewalls | NIDS | Web Proxy | SIEM | OpenIOC

APT Pyramid of Pain



GRIZZLY STEPPE – Russian Malicious Cyber Activity

CYBERSEER

U.S. Government refers to the Russian civilian and military intelligence service (RIS) responsible for the compromise and exploit of networks and endpoints associated with the U.S. election, as well as a range of U.S. Government, political, and private sector entities as GRIZZLY STEPPE.

- Linked to APT 28 & APT 29
- Targets Include:
  - Government
  - Critical Infrastructure
  - Think tanks
  - Universities
  - Political organisation's

IoCs in Action – GRIZZLY STEPPE

APT28 and APT29 activity from 2015 through 2016

CYBERSEER

CYBER THREAT KILL CHAIN

Network Vuln. Scanning: 89.35.178.104

876 IPs

In attacker space/no IOC

Spear-phishing: Subject: efax #100345

Vulnerabilities: CVE-2016-7855

OnionDuke Malware: 8F154D23AC2071D7F179959AABA37AD5

C&C: Private.directinvesting.com

OnionDuke Malware: 8F154D23AC2071D7F179959AABA37AD5

The Problem with IoCs

CYBERSEER

- Single dimension
  - SIEM/OpenIOC overcomes this
- Known bad only
- Lack context
- Reactive
- Valid for short period of time
- Attacks are polymorphic
- False Positives
- False sense of security
- Too many IoCs to Threat Hunt

IP Query Result:

IP Address:	89.35.178.104
Risk Level:	Low Risk
Description:	This IP address is occasionally used for sending Spam

89.35.178.104 IP address information

Geolocation

Country	RO
Autonomous System	60115 (SC Klass Systems Grup SRL)

Passive DNS replication

VirusTotal's passive DNS only stores address records. **The following domains resolved to the given IP address.**

2015-07-09 315andro.net

Latest detected URLs

Latest URLs hosted in this IP address **detected by at least one URL scanner or malicious URL dataset.**

5/68	2018-08-27 10:02:46	http://89.35.178.104/JP/loading.php
6/68	2018-08-23 06:19:43	http://89.35.178.104/allexe/alina111.exe
7/68	2018-08-22 21:49:40	http://89.35.178.104/allexe/jack111.exe
6/68	2018-08-21 22:06:31	http://89.35.178.104/insider/jack.exe
3/67	2018-08-15 05:00:31	http://89.35.178.104/
6/67	2018-08-08 02:42:38	http://89.35.178.104/www.intesasanpaolo.com/script/ServiceLogin/ib/login.html
4/67	2018-05-23 14:29:28	http://89.35.178.104/www.intesasanpaolo.com/script/ServiceLogin/ib
2/64	2017-04-13 15:50:59	http://89.35.178.104/www.intesasanpaolo.com/script/ServiceLogin/ib/
4/64	2017-03-20 11:28:36	http://89.35.178.104/insider/64.exe
2/68	2016-07-19 17:53:18	https://89.35.178.104/

Detecting Threats with IoCs

Doesn't scale with traditional SIEM

CYBERSEER

- Hope you're not patient 0
- IoCs from every security vendor
- Correlation rules = IoCs
- Causes alert fatigue
- Rarely does IoC = compromise
  - How would you know?

Aug 27th 2018, 21:54:26.122

SECURITY ALERTS

user steve alert_name trojan alert_type security advanced malware command and control src_ip 10.10.3.172 src_host - malware_url -

host localhost

<190>Aug 28 04:54:24 localhost "loc=989411|time=31Oct2016 08/28/2018 04:54:20 AM|action=drop|orig=10.10.3.146|i/f_dir=inbound|i/f_name=eth2-01.75|has_accounting=0|uuid= <00000000,00000000,00000000,00000000>|product=SmartDefense|Protection Name=trojan|Severity=LOW|Confidence Level=0|protection_id=BlockByCountries|SmartDefense Profile=Internet_Protection|Performance Impact=2|Protection Type=geo_protection|src_country=United States|dst_country=United States|Attack Info=security advanced malware command and control|attack=Geo-location enforcement|src=10.10.3.172|s_port=53288|dst=10.10.0.40|service=443|proto=tcp|user= (steve)(+)|src_user_name= (steve)(-)|snid=3c423261|__policy_id_tag=product=VPN-1 & FireWall-1[db_tag={82BB8CE7-409E-5840-AED6-33317536F258};mgmt=dayprdchkptmgt01;date=1477908212;policy_name=Standard]|origin_sic_name=10.10.3.146" Collapse

alert_type: security advanced malware command and control | exa_adjustedEventTime: Oct 31st 2016, 03:03:32.000 | alert_severity: LOW | exa_category: Security Alerts | src_ip: 10.10.3.172 | exa_rawEventTime: Oct 31st 2016, 03:03:32.000 | @version: 1 | host: localhost | exa_parser_name: s-checkpoint-alert | dest_port: 443 | dst_country: United States | indexTime: Aug 27th 2018, 21:54:26.122 | exa_activity_type: alert/security, alert | Vendor: Check Point ThreatCloud | src_port: 53,288 | exa_device_type: security | @timestamp: Aug 27th 2018, 21:54:26.109 | port: 49364 | src_country: United States | dest_ip: 10.10.0.40 | forwarder: 10.0.1.117 | data_type: alert | time: Oct 31st 2016, 03:03:32.000 | user: steve | alert_name: trojan | _id: AWV-4gRKJhjrjb4aAcgp | _type: logs | _index: exabeam-2018.08.28 | _score: - |

BUILD RULE

BUILD
BLACKLIST

Trigger if the value of

DEST_IP is in the list of

85.13.122.41,
121.42.41.56

Not sure what to do?
Choose from Examples

Responding to IoCs

Doesn't scale with traditional SIEM

CYBERSEER

SEARCH VISUALIZE DASHBOARDS

dest_ip:"251.251.81.175" | Filter by Time: Last 7 days | Refresh Rate | SAVE | LIBRARY

August 20th 2018 22:06:00:952 -0700 → August 27th 2018 22:06:00:952 -0700 Time View

Count: 1, 0.8, 0.6, 0.4, 0.2, 0

2018-08-21 05:00 | 2018-08-22 05:00 | 2018-08-23 05:00 | 2018-08-24 05:00 | 2018-08-25 05:00 | 2018-08-26 05:00 | 2018-08-27 05:00

indexTime

SECURITY ALERTS
- alert_name (1)
- alert_type (1)
- host (1)
- src_ip (1)
- user (1)

DEFAULT
- @timestamp (1)
- @version (1)
- alert_name (1)
- alert_severity (1)
- alert_type (1)

LOG VIEW: ENHANCED TABLE RAW | Share | Export

Sort by Time | 1 hit

Aug 27th 2018, 18:56:00.474

SECURITY ALERTS

user eric | alert_name security advanced malware command and control | alert_type security advanced malware command and control | src_ip 192.168.2.16

src_host - | malware_url - | host localhost

<190>Aug 28 01:55:39 localhost "loc=989411|time=31Oct2016 08/28/… View all

exa_adjustedEventTime: Oct 31st 2016, 03:03:32.000 | alert_severity: 3 | exa_category: Security Alerts | alert_type: security advanced malware command and control | src_ip: 192.168.2.16 | exa_rawEventTime: Oct 31st 2016, 03:03:32.000 | @version: 1 | host: localhost | exa_parser_name: s-checkpoint-alert | dest_port: 443 | dst_country: China | indexTime: Aug 27th 2018, 18:56:00.474 | exa_activity_type: alert/security, alert | Vendor: Check Point ThreatCloud | src_port: 53,288 | exa_device_type: security | @timestamp: Aug 27th 2018, 18:56:00.461 | port: 49364 | src_country: Sweden | dest_ip: 251.251.81.175 | forwarder: 10.0.1.117 |

dest_ip:"251.251.81.175" OR eric OR 192.168.2.16

August 26th 2018 22:07:44:459 -0700 → August 27th 2018 22:07:44:459 -0700 Time View

Count: 40,000, 30,000, 20,000, 10,000, 0

23:00 | 02:00 | 05:00 | 08:00

indexTime

AUTHENTICATION
- dest_host (246)
- dest_ip (609)
- event_code (2)

LOG VIEW: ENHANCED TABLE RAW

Sort by Time

500 of 1,462,776 hits

dest_ip:"251.251.81.175" OR eric OR 192.168.2.16

August 20th 2018 22:08:41:492 -0700 → August 27th 2018 22:08:41:493 -0700 Time View

Count: 200,000, 150,000, 100,000, 50,000, 0

2018-08-21 17:00 | 2018-08-22 17:00 | 2018-08-23 17:00

AUTHENTICATION
- dest_host (264)
- dest_ip (613)
- event_code (2)

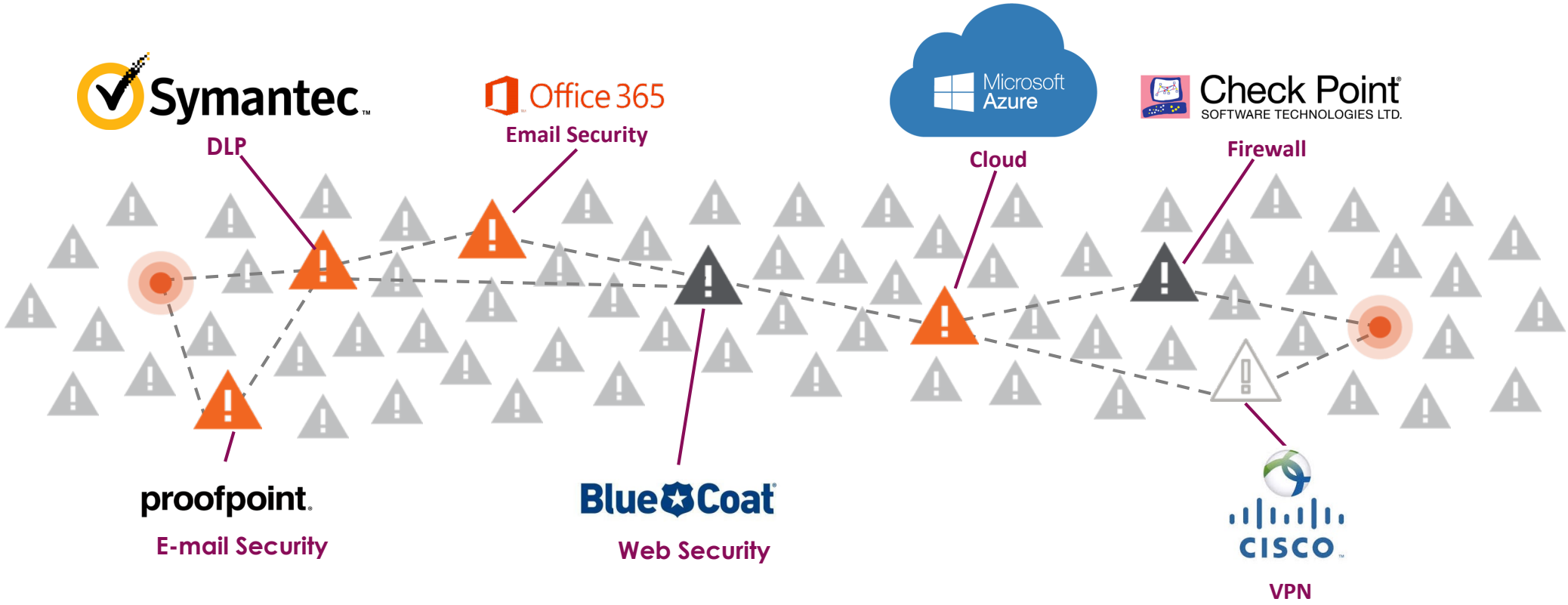
LOG VIEW: ENHANCED

Sort by Time

500 of 5,533,823 hits

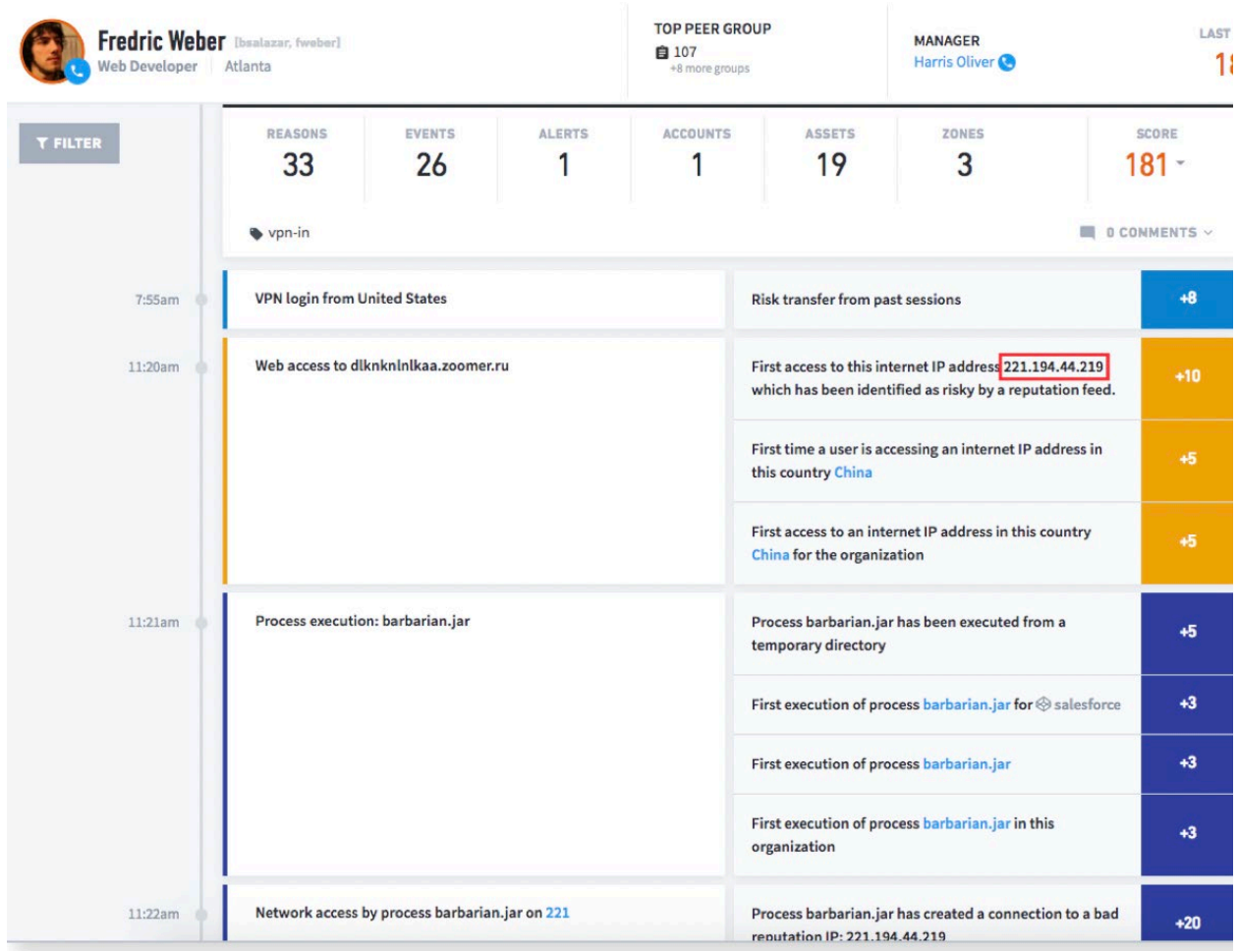
Complex Threats Span An Entire Organisation And Leave IOCs Behind

CYBERSEER



Scale IoCs with UEBA

CYBERSEER



What is a TTP?

CYBERSEER

Tactics, Techniques, and Procedures (TTP) are "**descriptive**" in nature and are for characterizing the how and what of adversary behavior (what they are doing and how they are doing it). They are abstracted from specific observed instances within individual specific Incidents so that they may be more generally applicable in developing contextual understanding across Incidents, Campaign and Threat Actors.

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 Interference	AppCert DLLs	AppCert DLLs	Binary Padding	Brute Force	Browser Bookmark Discovery	Distributed Component Object Model	Clipboard Data	Data Encrypted	
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 Staged	Data Transfer Size Limits	Custom Command and Control Protocol

**Mitre ATT&CK Technique Matrix

Persistence

Create Account

CYBERSEER

- Adversaries with a sufficient level of access may create a local system or domain account. Such accounts may be used for persistence that do not require persistent remote access tools to be deployed on the system.

- **Detection:** Collect data on account creation within a network. Event ID 4720 is generated when a user account is created on a Windows system and domain controller. Perform regular audits of domain and local system accounts to detect suspicious accounts that may have been created by an adversary.

Examples

- APT3 has been known to create or enable accounts, such as `support_388945a0`. [1]
- Dragonfly created accounts that appeared to be tailored to each individual staging target.[2]
- Flame can create backdoor accounts with the login "HelpAssistant" with the Limbo module.[3]
- Mis-Type may create a temporary user on the system named "Lost_{Unique Identifier}."[4]
- The `net user username \password` and `net user username \password \domain` commands in Net can be used to create a local or domain account respectively.[5]
- Pupy can user PowerView to perform "net user" commands and create local system and domain accounts.[6]
- S-Type may create a temporary user on the system named "Lost_{Unique Identifier}" with the password "pond~!@6"{Unique Identifier}."[4]

Challenge with TTPS

Attacker techniques hide in plain sight

CYBERSEER

- Brute Force
- RDP
- PowerShell
- Account Creation
- Process Discovery
- Data Compression
- FTP

TTPs + Analytics Cuts Through the Noise

Catching the red team red handed!

CYBERSEER

Red team compromised domain admin

- Created new credentials
    - Tactic: persistence
    - Technique: account creation

SIEM correlation rule to detect TTP

- Alert on any account creation
    - Can't whitelist DAs
    - DAs perform 95% of account creation

Analytics + TTPs

- Abnormal account creation from asset
- Abnormal account creation from network zone (IP phone network)

TTPs + Analytics No Longer Reactive

CYBERSEER

APT 3 Techniques	Behavioral Anomalies
Scheduled Task - An APT3 downloader creates persistence by creating the following scheduled task: schtasks /create /tn "mysc" /tr C:\Users\Public\test.exe /sc ONLOGON /ru "System".	• First service installation on host • Non-Privileged user created a scheduled task/service on privileged asset • Service created to execute a sensitive process (ie. Powershell) • Unusual process for service • Unusual service name in the org
Uncommonly Used Port - An APT3 downloader establishes SOCKS5 connections to two separate IP addresses over TCP port 1913 and TCP port 81	• Abnormal inbound connection on port for zone • Abnormal inbound network connection to this port for asset • Abnormal outbound connection on port for zone • First failed outbound connection on port for asset • First inbound/outbound connection on port for asset
PowerShell - APT3 has used PowerShell on victim systems to download and run payloads after exploitation.	• First/Abnormal execution of PowerShell process for user/peer/org • Encrypted argument in PowerShell command detected
Remote Desktop Protocol - APT3 enables the Remote Desktop Protocol for persistence	• First/abnormal remote logon to asset for user/peer • First remote logon to asset for group by NEW user • Remote logon to private asset for new user
Create Account - APT3 has been known to create or enable accounts, such as support_388945a0	• First/abnormal account creation activity for user/peer • Abnormal time to perform account management activity for user/peer/org

TTP's in Action – GRIZZLY STEPPE

CYBERSEER

CYBER THREAT KILL CHAIN

Network Vuln. Scanning:
Abnormal inbound connection from country

In attacker space/no IOC

Spearphishing attachment
First email domain for Org

Exploitation for Client Execution:
Abnormal number of critical windows command executions by user

Web Shell
First execution of process in this directory for Org

C&C:
First web activity to this country for Org

Data Transfer Size Limits:
Abnormal amount of data uploaded to web for Org

Risk Fabric Revisited

CYBERSEER

Tactic: Lateral Movement
Technique: RDP

Tactic: Privilege Escalation
Technique: Valid Accounts

Tactic: Persistence
Technique: Account Creation

exabeam

Search for Users and Assets

Julietta Donaldson [jdonaldson, bsalazar, jdonaldson-admin, achen]
IT Administrator | Chicago

TOP PEER GROUP
IT
+8 more groups

MANAGER
Felipe Pennington

LAST SCORE
242

FILTER

1:43pm	Remote logon to sfo_term_23	Suspicious NTLM Logon from unrecognized asset eow8age4vljuk6f2. Possible pass-the-hash attack	+80
		First time user is performing an activity from North Korea	+20
		First activity from ISP Ryugyong-dong	+15
		First activity from country North Korea for group IT	+12
		First activity from country North Korea for organization	+10
		First remote logon to sfo_term_23 for Julietta Donaldson	+7
2:04pm	Remote logon to cal-ad-003	First remote logon to cal-ad-003 for Julietta Donaldson	+7
2:04pm	Account switch to jdonaldson-admin on sfo_term_23	Credential switch to a privileged or executive account jdonaldson-admin	+40
2:13pm	Created zerocool's account on cal-ad-003	First account management activity from asset cal-ad-003	+20
		First account management activity from asset cal-ad-003 for user Julietta Donaldson	+20
		Abnormal account creation on domain ktenergy for	

IOC vs TTP

CYBERSEER

IOCs

- 100s of millions
- Constantly changing
    - Can change within an attack
- Focus of todays detections
    - Signatures
    - Correlation Rules
- Threat hunting starts with IOCs

TTPs

- 291 TTPs ATT&CK Framework
- Rarely change
    - No need to develop new TTPs attackers are successful
- Detection moving to TTPs
    - Correlation Rules
    - Behavior*
- Hard to Threat Hunt behavior in legacy SIEM

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control

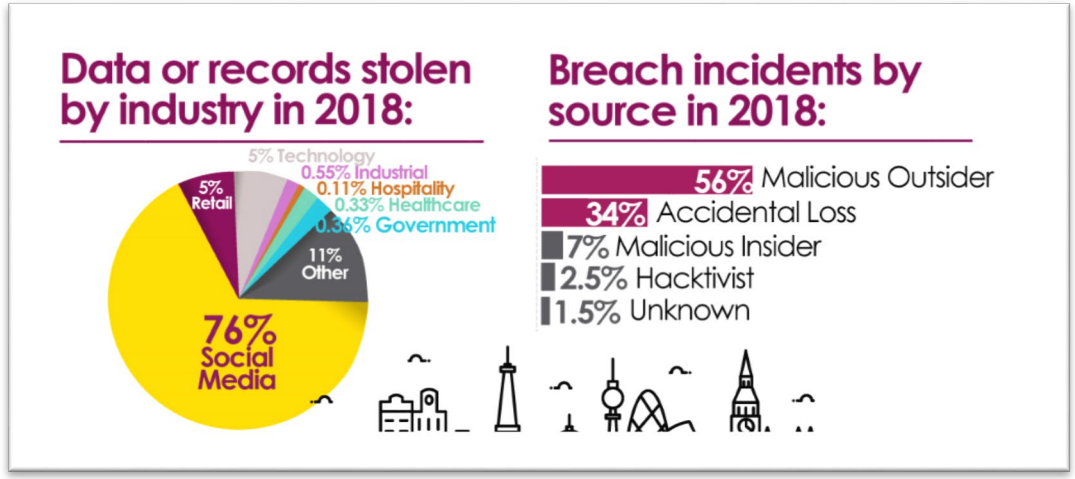
Future of Threat Hunting is TTP Based

CYBERSEER

- **Cast a wider net**
  - TH can start broad
  - Start with a question "has anyone done X"
  - Easily filter out the normal
- **Identify parts of the kill chain through TTPs**
- **Create APT* based detection**
- **Answers the expensive questions**
- **You might stumble on IoCs**
- **Hunt for the unknown**
  - DGA

Cyber Stats 2018

CYBERSEER



For the full infographic visit:

https://www.cyberseer.net/infographic/

Cyber Predictions 2019

CYBERSEER

Advanced Threat Detection

CYBERSEER

T: 0203 823 9030
E: info@cyberseer.net
W: www.cyberseer.net