Cyber Threat Hunting

Tracking Your Adversaries

Brent King

Agenda

What is Threat Hunting?

Why Threat Hunt?

What are the Tools for Hunting?

What Threats to Hunt for?

Summary

Q & A

What is Threat Hunting?

Threat Hunting

PROACTIVELY and METHODICALLY searching for potential threats within your organizations computer systems and networks.

Why Threat Hunt?

Why Threat Hunt?

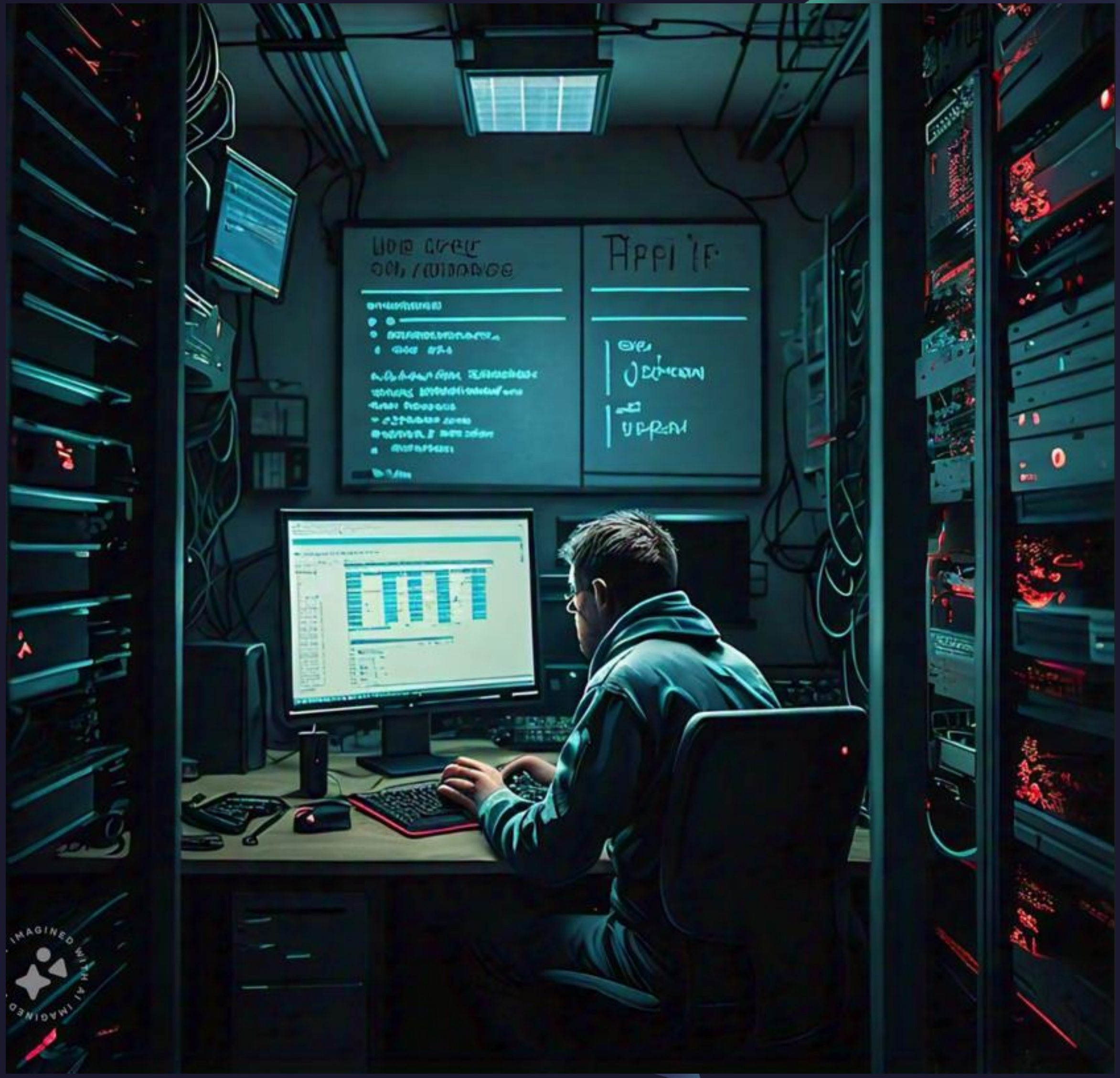
- PREPARE TO BE COMPROMISED, skilled adversaries will get in eventually, be ready!
- Practice your ability to search your telemetry for malicious behavour.
- Threat Hunting reveals new detection methods and missing log sources.
- Improve the configuration of your security tools.
- Forces security team to learn the environment which will make your team more effective when a security event happens.

Precursors to Threat Hunting

1. Know your environment (Baseline):
   - VPN, perimeter access points
   - Crown Jewels
   - Typical Commands, Processes, Services, Software, Scripts
   - Remote admin tools
   - Administrators
2. Know your toolsets, data sources available to you
   - What are my key toolsets?
   - Do I have access to them?
   - Do I know how to use them?

Threat Hunting Process

1. Scope - Define your hunt mission
2. Hunt – Search for your adversary
3. Analyze - compare your results against your baseline
4. Action - Determine impact and take actions
5. Improve - Review your defenses, log sources, and tooling for future hunts



What Threat Hunting Tools?

Threat Hunting Tools

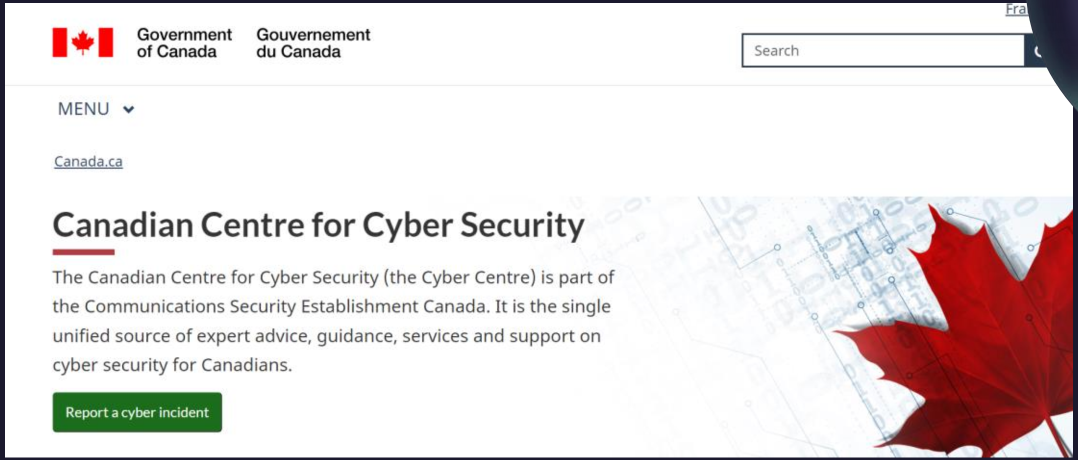
- Threat Intelligence/Advisories
- MITRE Att&ck Framework
- EDR – Endpoint Detection and Response
- SIEM/Log Management tools
- Network Management Systems (flows, connections., PCAP)
- Web Access/Proxy
- IAM/Active Directory

Top Telemetry and Data Sources

- Security Alerts
- Process Execution
- Command Shell
- Script Execution
- Registry Changes
- Remote Admin Tool
- File Read/Write
- URL access
- DNS
- IP Connectivity/Netflow

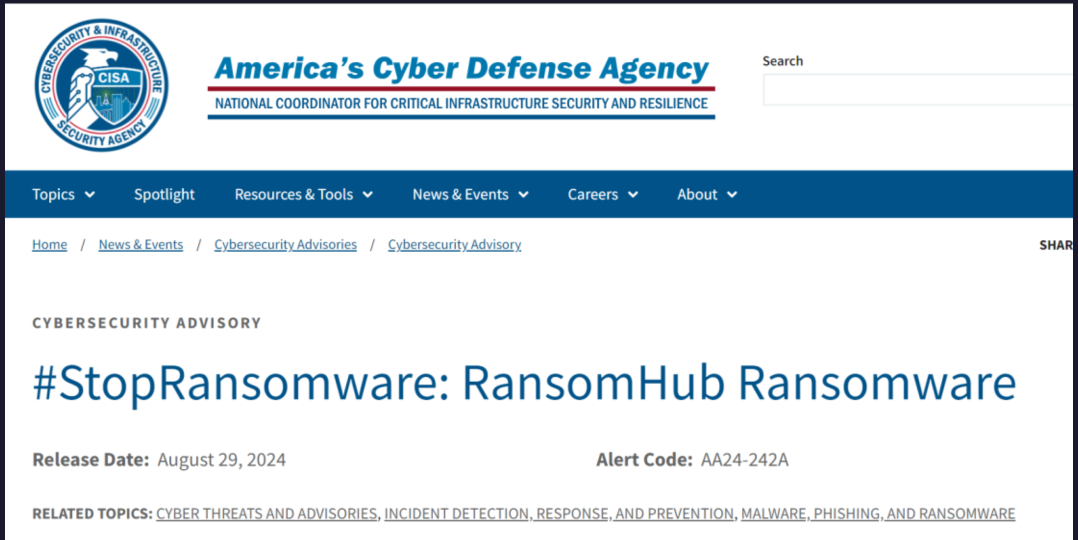
What Threats to Hunt for?

Threat Advisories & Intel Reports



Canadian Centre for Cyber Security

The Canadian Centre for Cyber Security (the Cyber Centre) is part of the Communications Security Establishment Canada. It is the single unified source of expert advice, guidance, services and support on cyber security for Canadians.


CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY
CISA
America's Cyber Defense Agency
NATIONAL COORDINATOR FOR CRITICAL INFRASTRUCTURE SECURITY AND RESILIENCE
Search
Topics
Spotlight
Resources & Tools
News & Events
Careers
About
Home / News & Events / Cybersecurity Advisories / Cybersecurity Advisory
SHAR

CYBERSECURITY ADVISORY

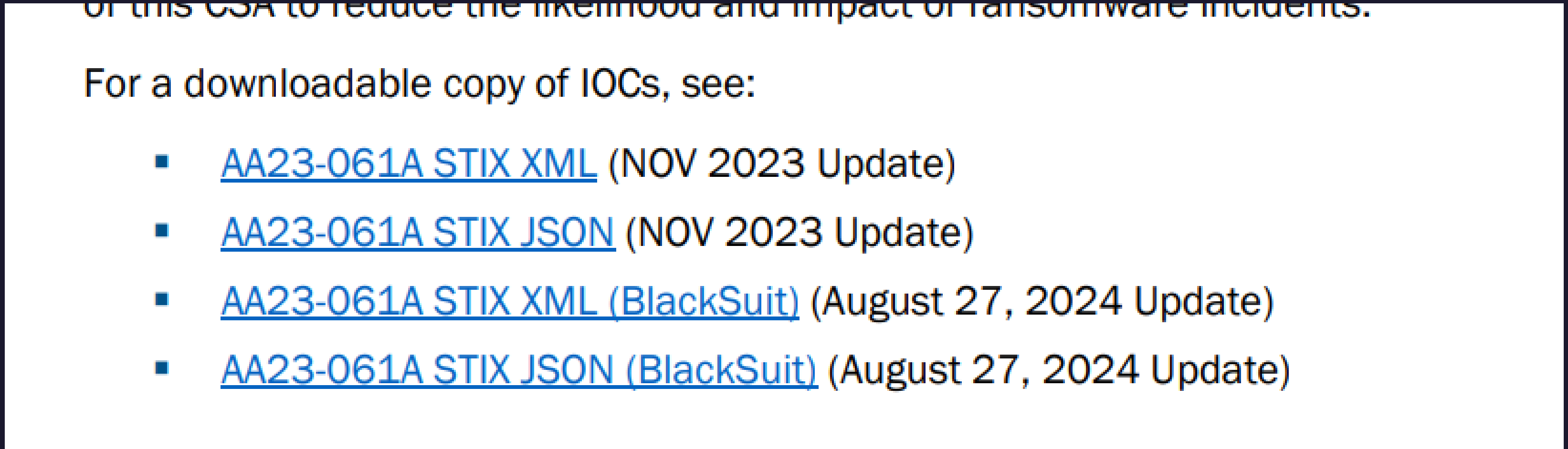
#StopRansomware: RansomHub Ransomware

Release Date: August 29, 2024

Alert Code: AA24-242A

RELATED TOPICS: CYBER THREATS AND ADVISORIES, INCIDENT DETECTION, RESPONSE, AND PREVENTION, MALWARE, PHISHING, AND RANSOMWARE

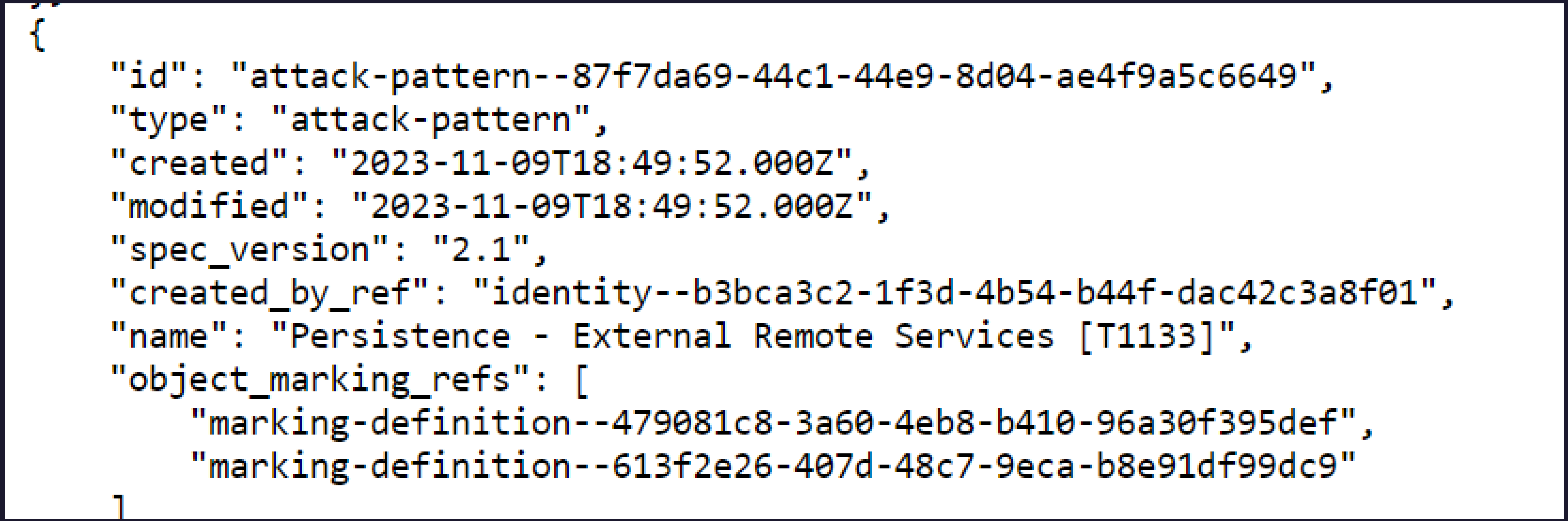
Indicators of Compromise (IoC)



of this CSA to reduce the likelihood and impact of ransomware incidents.

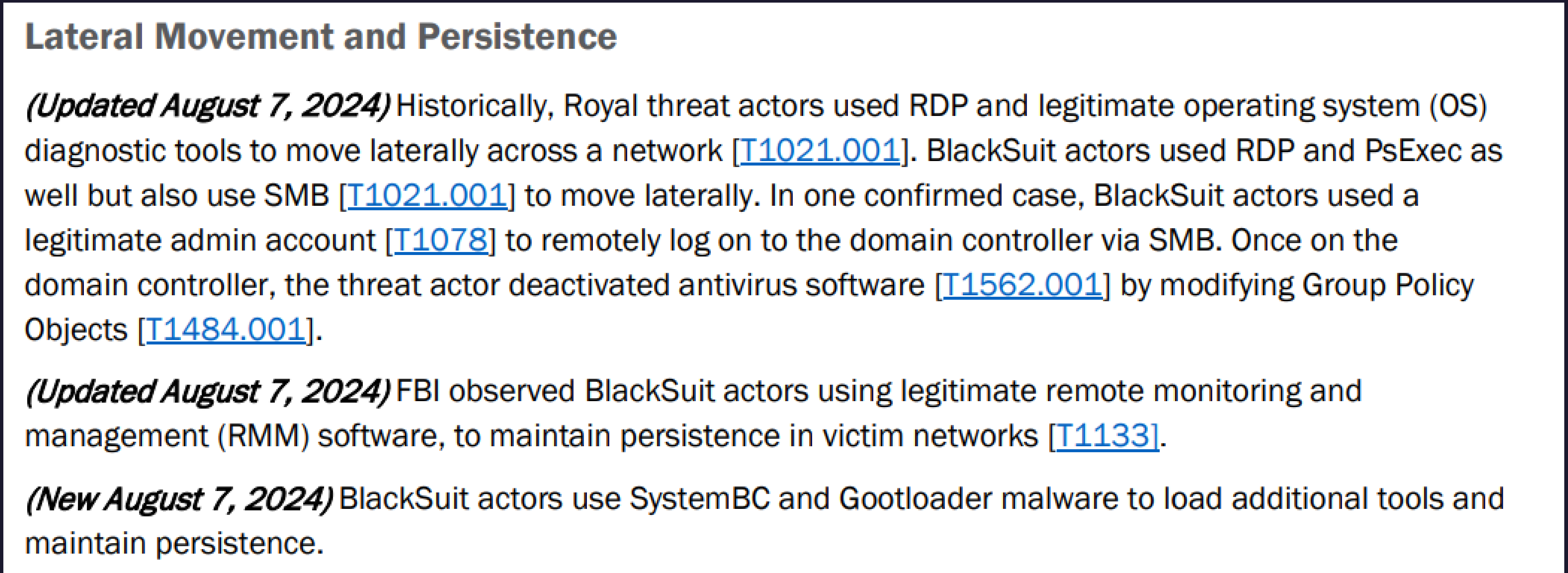
For a downloadable copy of IOCs, see:

- AA23-061A STIX XML (NOV 2023 Update)
- AA23-061A STIX JSON (NOV 2023 Update)
- AA23-061A STIX XML (BlackSuit) (August 27, 2024 Update)
- AA23-061A STIX JSON (BlackSuit) (August 27, 2024 Update)



```
},
{
    "id": "attack-pattern--87f7da69-44c1-44e9-8d04-ae4f9a5c6649",
    "type": "attack-pattern",
    "created": "2023-11-09T18:49:52.000Z",
    "modified": "2023-11-09T18:49:52.000Z",
    "spec_version": "2.1",
    "created_by_ref": "identity--b3bca3c2-1f3d-4b54-b44f-dac42c3a8f01",
    "name": "Persistence - External Remote Services [T1133]",
    "object_marking_refs": [
        "marking-definition--479081c8-3a60-4eb8-b410-96a30f395def",
        "marking-definition--613f2e26-407d-48c7-9eca-b8e91df99dc9"
    ]
```

Tactics, Techniques and Procedures (TTPs)



Lateral Movement and Persistence

(Updated August 7, 2024) Historically, Royal threat actors used RDP and legitimate operating system (OS) diagnostic tools to move laterally across a network [T1021.001]. BlackSuit actors used RDP and PsExec as well but also use SMB [T1021.001] to move laterally. In one confirmed case, BlackSuit actors used a legitimate admin account [T1078] to remotely log on to the domain controller via SMB. Once on the domain controller, the threat actor deactivated antivirus software [T1562.001] by modifying Group Policy Objects [T1484.001].

(Updated August 7, 2024) FBI observed BlackSuit actors using legitimate remote monitoring and management (RMM) software, to maintain persistence in victim networks [T1133].

(New August 7, 2024) BlackSuit actors use SystemBC and Gootloader malware to load additional tools and maintain persistence.

Cyber Threat Actor Toolset

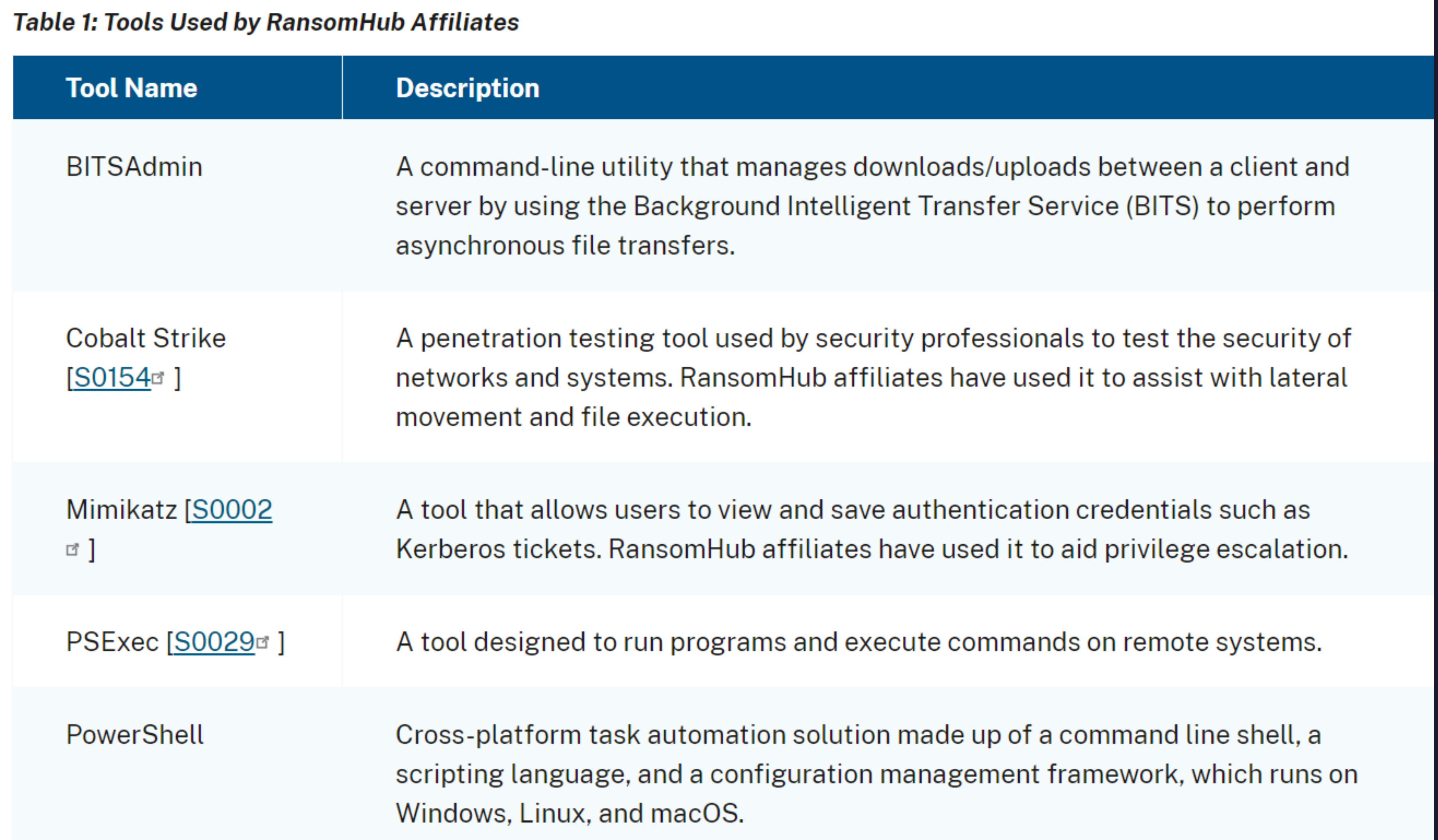
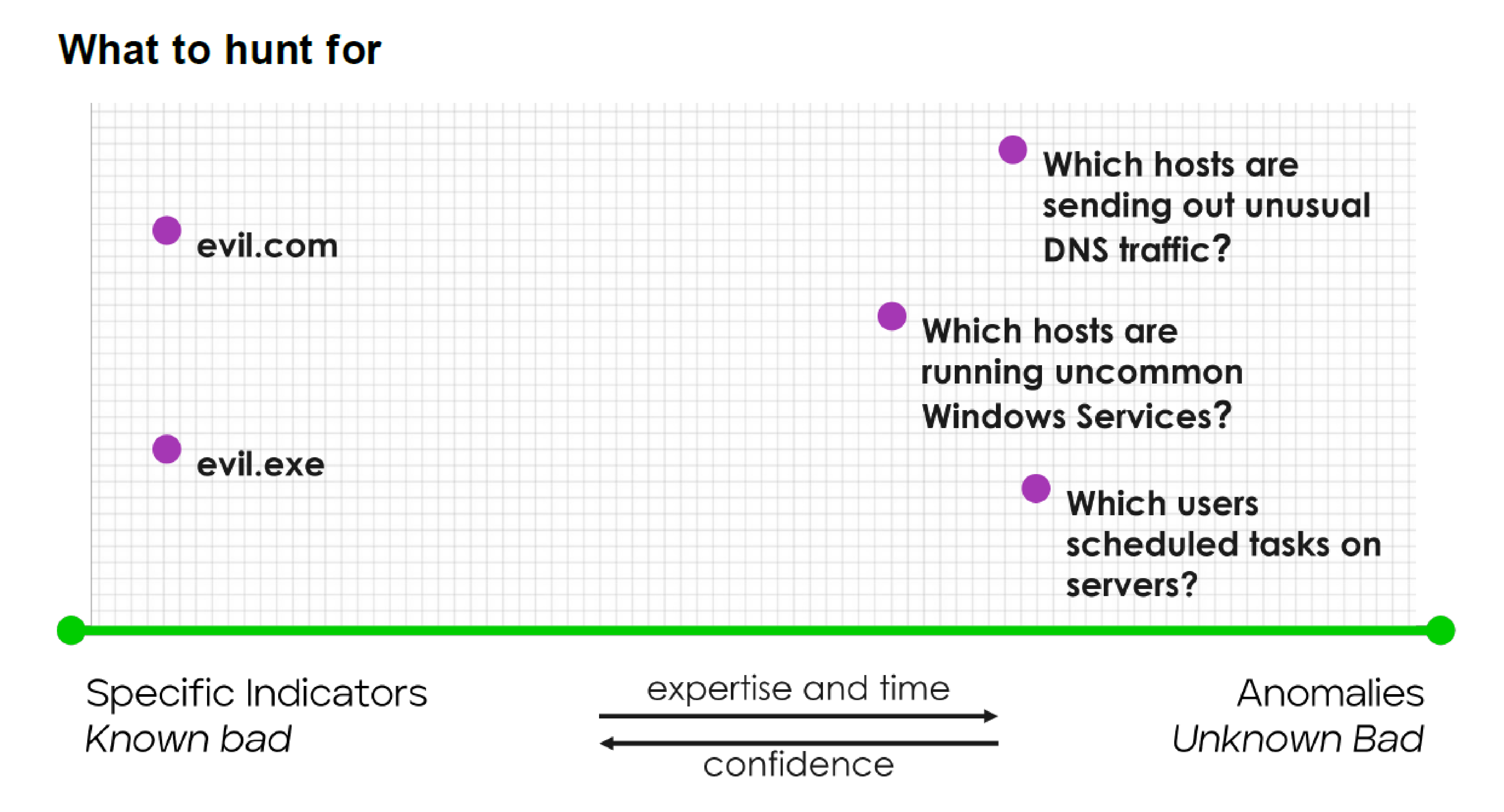


Table 1: Tools Used by RansomHub Affiliates

Tool Name	Description
BITSAdmin	A command-line utility that manages downloads/uploads between a client and server by using the Background Intelligent Transfer Service (BITS) to perform asynchronous file transfers.
Cobalt Strike [S0154]	A penetration testing tool used by security professionals to test the security of networks and systems. RansomHub affiliates have used it to assist with lateral movement and file execution.
Mimikatz [S0002]	A tool that allows users to view and save authentication credentials such as Kerberos tickets. RansomHub affiliates have used it to aid privilege escalation.
PSExec [S0029]	A tool designed to run programs and execute commands on remote systems.
PowerShell	Cross-platform task automation solution made up of a command line shell, a scripting language, and a configuration management framework, which runs on Windows, Linux, and macOS.

What to Hunt for?



What to hunt for

evil.com

evil.exe

Which hosts are sending out unusual DNS traffic?

Which hosts are running uncommon Windows Services?

Which users scheduled tasks on servers?

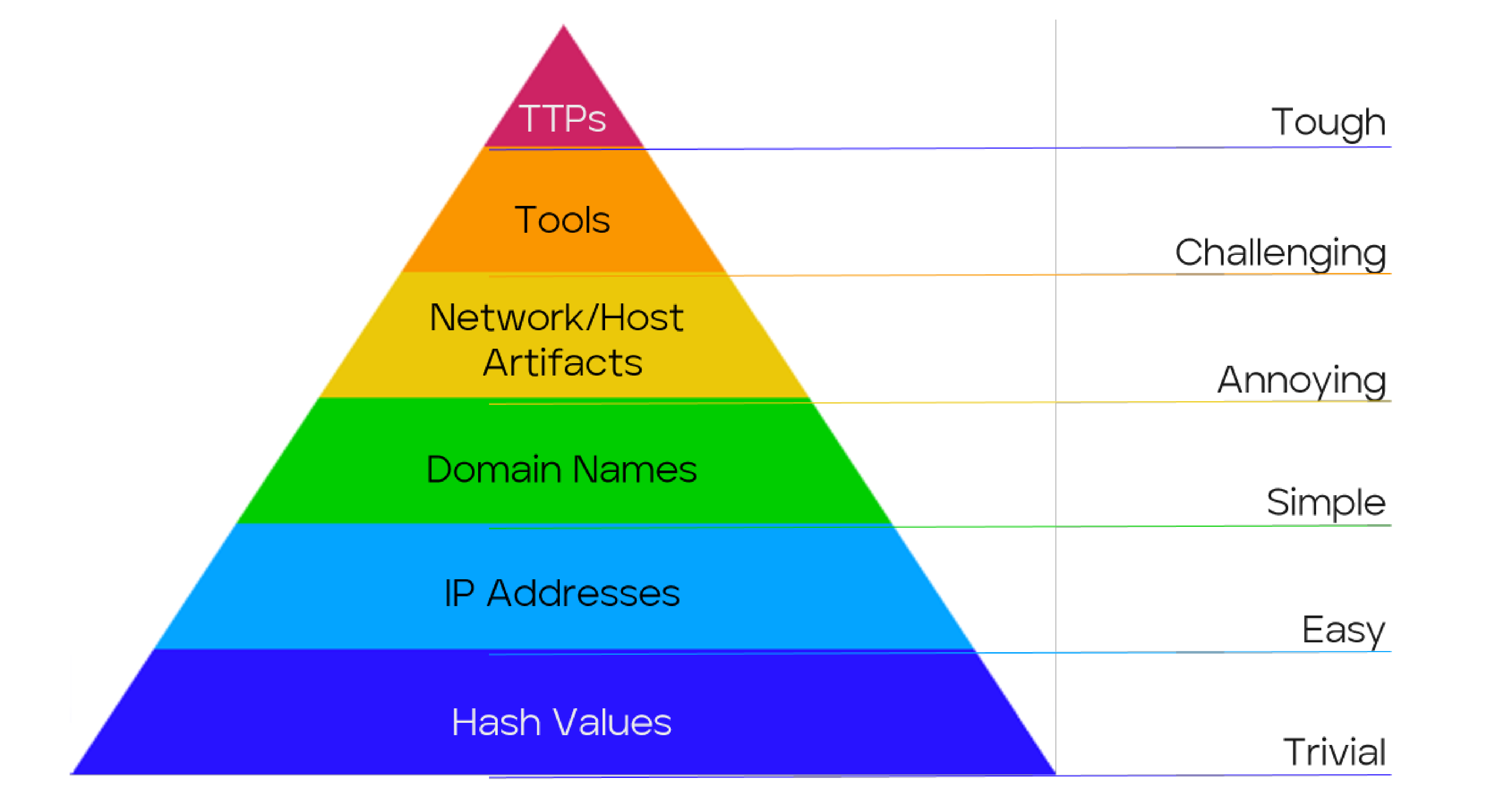
Specific Indicators
Known bad

expertise and time →

← confidence

Anomalies
Unknown Bad

What to Hunt for?



Summary and Q & A

Thank you

Brent King