



Incident Management in 'Sherlock' Mode: Close-loop Threat Detection & Response



Andrew Morrisett
Qualys Product Management

A day in the life of a SOC analyst

Outlook

Search

Home View Help

New email Delete Archive Report Sweep Move to Reply Read / Unread

Endpoint Detection and Response has detected malware Ransomhub on Asset ATLISSIAN-CONF-01

Intelligence SOC Team <intelligence@acme.com>
To: Analyst Team - L1

This message is on high priority

Hi Andrew,

Endpoint Detection and Response has detected **malware Ransomhub-0987** on **Asset ATLISSIAN-CONF-01** on Wednesday October 9th, 5:26pm
Malware was detected on an asset.

Malware Details
Threat Details: Exploit CVE-2023-22515
Threat Score: 10
mitre.attack.tactic.name: "Initial Access"
mitre.attack.group.name: ["Ransomhub","Storm-0062","C3RB3R"]

User Details
Name: AS-1 Admin
Username: Admin
Department: Infra-P0

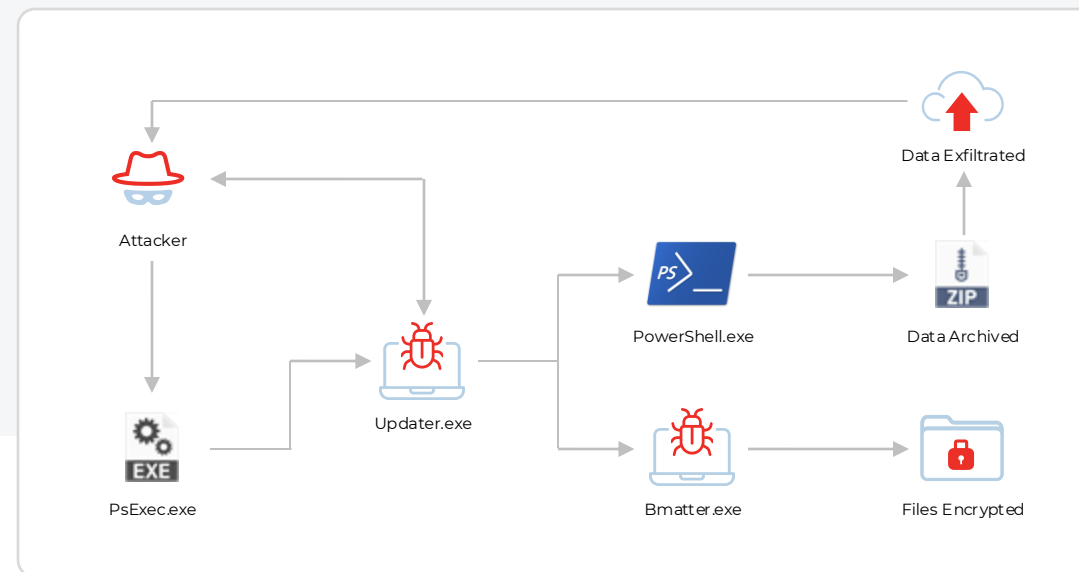
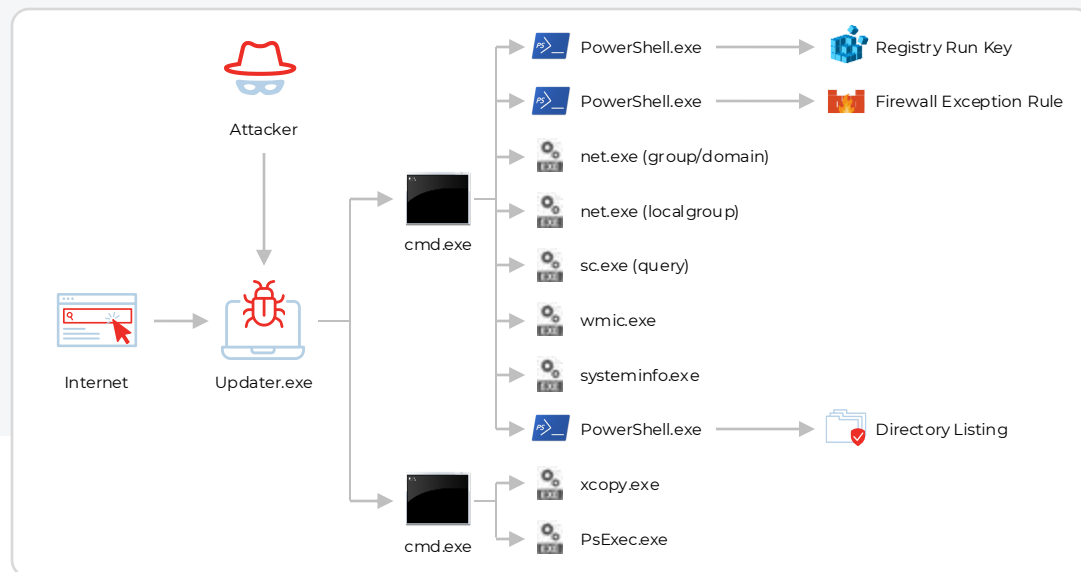
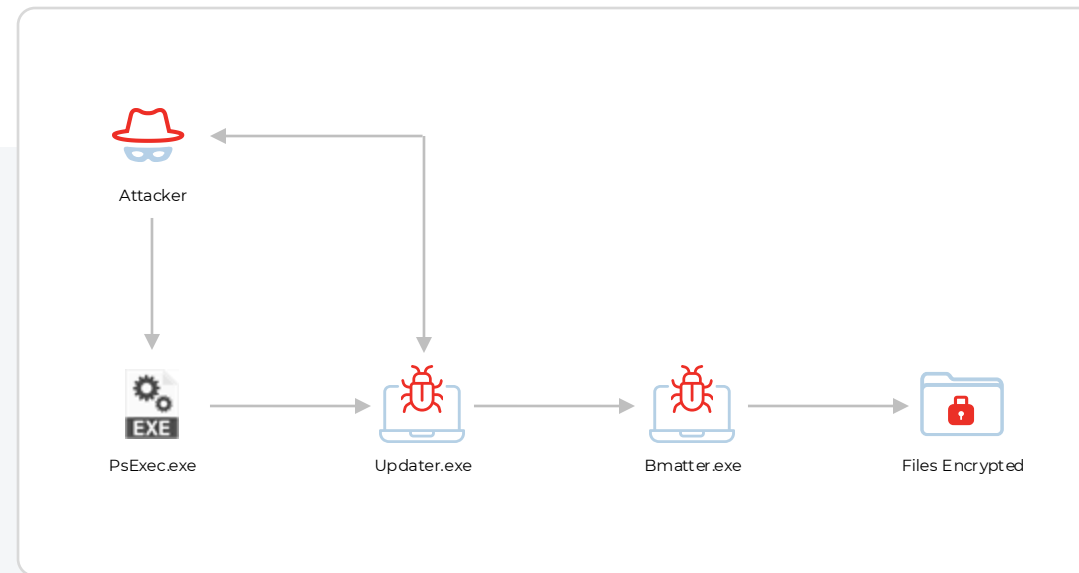
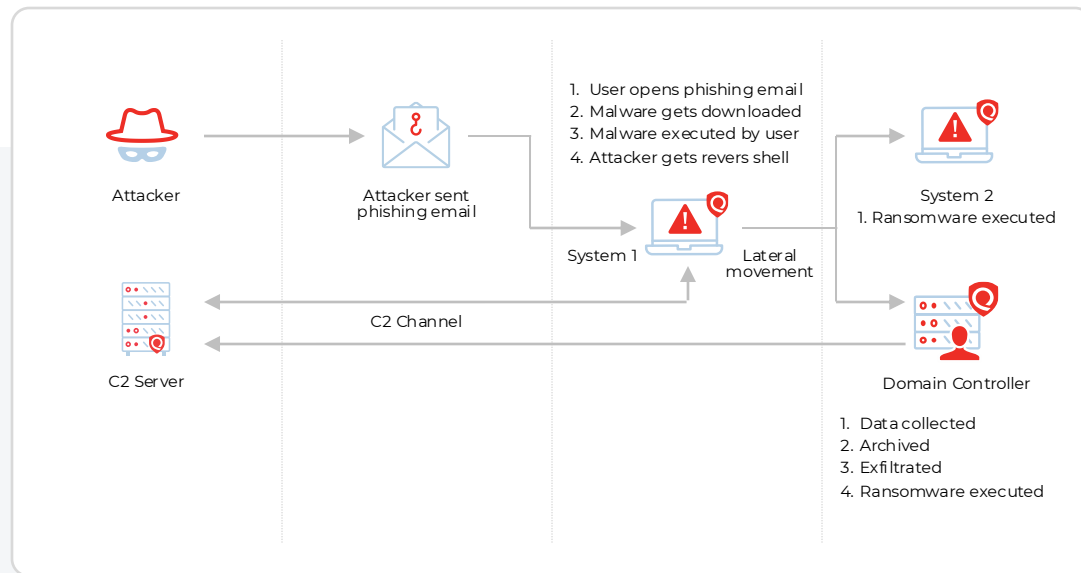
Asset Details
Host Name: ATLISSIAN-CONF-01
Asset Criticality: 5
IP Address: 172.16.197.89
Operating System: Windows Server 2019

Qualys Endpoint Protection

You are at risk
1 ISSUE FOUND >

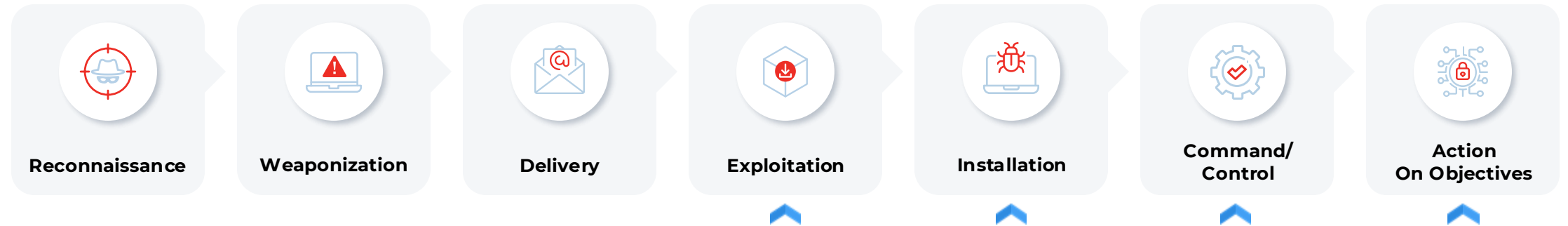
Event log:

- Antimalware** 23 Jan, 14:33
Ransomware Mitigation has blocked a ransomware attack. Origin: C:\KB4\Newsim\DataDir\MainFolders\6\1008274268.cxr. Threat name: atc.heur.crypt.
- Antimalware** 23 Jan, 14:33
Advanced Threat Control has detected a process as malicious. No action was taken. Process path: C:\KB4\Newsim\DataDir\MainFolders\6\1008274268.cxr. Threat name: ATC.SuspiciousBehavior.6B67707E265C55FA. To block malicious processes, please contact your system administrator.
- Antimalware (2)** 23 Jan, 14:33
Ransomware Mitigation has blocked a ransomware attack.

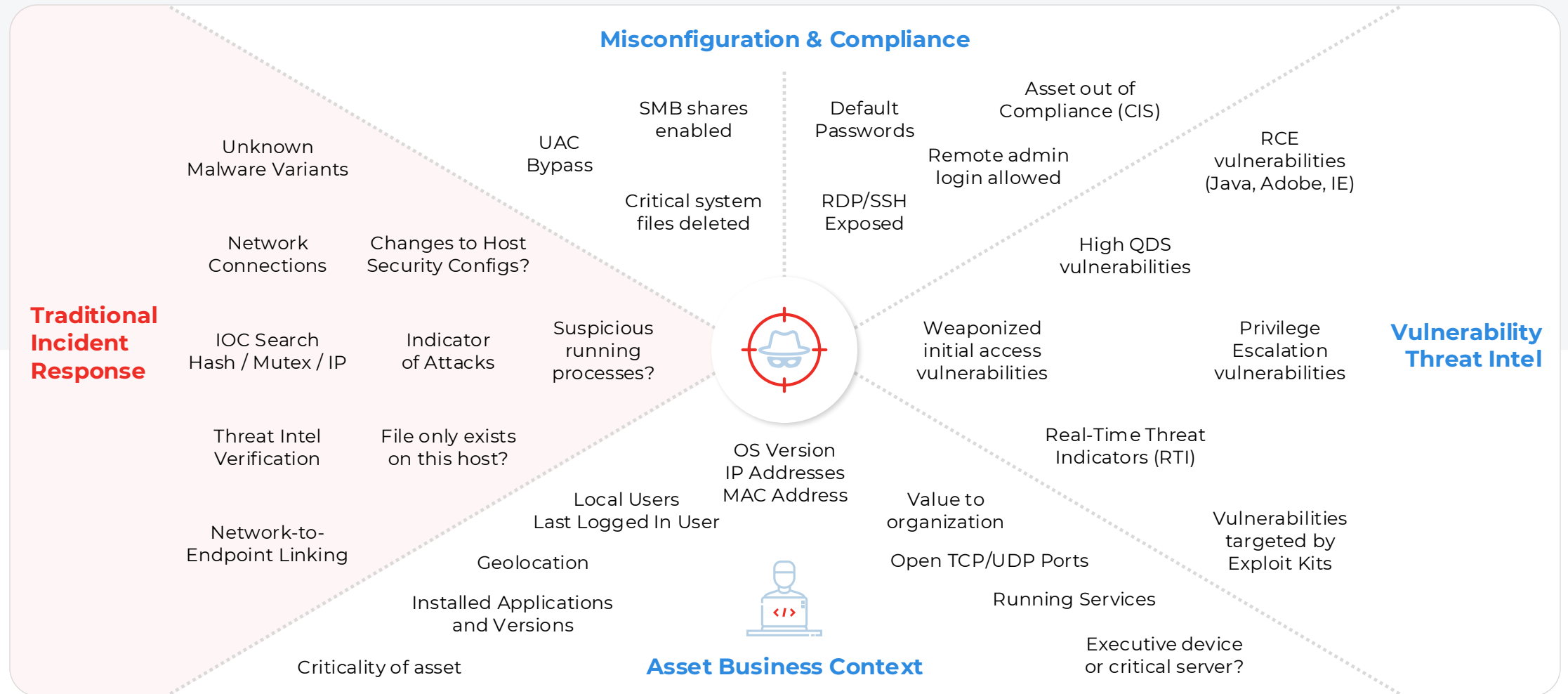


Rethinking Incident response

Thinking like an Attacker



More to consider



**How does your team have
unified risk elimination before,
during, and after an attack?**



Need for Risk-based Approach for Endpoint Security

DE-RISK YOUR BUSINESS

Qualys Cloud Platform

← Incident Details: Ransomhub

VIEW MODE

Summary

Timeline

Process Tree


Risks and Exploits

Comments

Activity Log

Affected Files

Risks and Exploits

 **Ransomhub** activity detected

Incident Number: 57104 | Asset Name: ATLISSIAN-CONF-01 | Status: Open | Severity Score 10

THREAT RISK & EXPOSURE

SYSTEM MISCONFIGURATIONS


CSAM

Malware Impacted Hosts (7)

Shows list of malware(s) reported in the incident and the list of assets impacted by each malware (in last 7 days).

⚠ Please consider remediating the following vulnerabilities to avoid similar compromises in the future. These are targeted for exploitation by the threats detected in this incident.

☐ Patch Now

 Filter

Show Vulns:

All Hosts

Current Host

☒ Show only Patchable

QID	TITLE	CVE	MALWARE	TOTAL HOSTS	QDS
378674, 378681	Citrix ADC and Gateway Unauthenticated Remote Code Execution Vulnerability	CVE-2023-3519	QthAZN.exe	1	100
44059	Fortinet FortiOS and FortiProxy SSL-VPN Critical Heap-Based Buffer Overflow Vulnerability	CVE-2023-27997	CVE-2023-27997	2	100
150757	Apache ActiveMQ Remote Code Execution (RCE) Vulnerability	CVE-2023-46604	CVE-2023-46604	5	100
150725	Atlassian Confluence Data Center and Server Authentication Bypass Vulnerability	CVE-2023-22515	Ransom hub	1	100
91668, 91680	Microsoft Netlogon Elevation of Privilege Vulnerability ("Zerologon")	CVE-2020-1472	CVE-2020-1472	12	95
91360	Microsoft Windows SMBv1 Remote Code Execution Vulnerability ("EternalBlue")	CVE-2017-0144	CVE-2017-0144	6	95

AI is Automating Attacks



Phishing Attacks

LLMs generate convincing emails mimicking trusted sources to trick users into divulging sensitive information.



Social Engineering

LLMs assist attackers in crafting persuasive messages, social media posts, or chat interactions to manipulate targets.



Malware and Ransomware Creation

LLMs aid in generating code snippets, camouflage techniques, or obfuscation methods to create sophisticated malware.



Automated Vulnerability Exploitation

LLMs automate the process of identifying and exploiting vulnerabilities in software or networks.





AI needs to Automate Defense

AI Incident Summarization



Incident Summary

On September 23, 2024, the incident involved the termination of 'explorer.exe' by 'svchost.exe', which led to the execution of a batch file 'AdobeAcrobatReader.bat' using 'cmd.exe'. The batch file then invoked 'attrib.exe' multiple times to modify file permissions for the malicious document 'NatoDoc.pdf' and its associated link. The final event in the sequence was the execution of the malware 'CobaltStrike' from the file 'AdobeReader.exe'.



Event Timeline

Timeline of Detected Events :

- | | |
|-----------------------------------|--|
| September 23rd 2024
6:22:45 am | • [12516] explorer.exe is executed by svchost.exe
(/factory,{75dff2b7-6936-4c06-a8bb-676a7b00b24b} -Embedding) |
| September 23rd 2024
6:21:50 am | • [2908] cmd.exe is executed by explorer.exe
(/c ""C:\Users\admin\Desktop\19066736666\Test\CZ_army_NATO_cooperation\AdobeAcrobatReader.bat" |
| September 23rd 2024
6:21:52 am | • [5408] attrib.exe is executed by cmd.exe
(-r -s -h "C:\Users\admin\Desktop\19066736666\Test\CZ_army_NATO_cooperation\The importance of and outlook for the Czech Republic in NATO.pdf") |
| September 23rd 2024 | • [14356] attrib.exe is executed by cmd.exe |

Demo

