Infocyte Cloud™

Endpoint Assessment

Report

<<Company Name>>

Contents

Copyright and Acknowledgements

Infocyte Endpoint Threat Assessment Report

An Infocyte Endpoint Threat Assessment was conducted between January and February 2021 on behalf of <<Company Name>>, hereafter referred to as <<Company Name>>. The goal of this service was to detect, analyze, and report malicious objects, vulnerabilities, and potentially unwanted applications in <<Company Name>> sampled environment. An additional objective of this assessment was to rate the exposure resulting from the SolarWinds compromise, commonly known as Sunburst. Findings that were recognized as critical and immediate were communicated at the point of detection to authorized <<Company Name>> representatives by the Infocyte Security Operations Center. Immediate and non-immediate threats, vulnerabilities, and unwanted applications are also reported below—with or without prior notification to stakeholders.

Methodology

Infocyte's model for a proactive threat assessment is focused on rapid detection of malware, indicators of compromise, and artifacts of unauthorized activity using a proprietary threat hunting platform. After identification of a possible threat, we will make an early assessment of the object, risks, and scope of the possible compromise. Armed with this information, we enable organizational leaders to make prompt decisions related to business continuity and level of effort for a response.

Infocyte™ assesses each device (workstation and server) on the network, evaluating all running processes, services, and anything triggered or scheduled to run. Additionally, it looks at operating system configurations and searches volatile memory to detect signs of manipulation that could indicate hidden rootkit activity or signs of compromise. When suspicious executables are found, it uses multiple 3rd party anti-malware and detection engines, plus proprietary malware analysis on the backend, to identify unknown ("zero-day") malware.

When responding to discovered incidents we may employ various lower-level forensics and incident response tools such as Access Data's FTK™, Guidance Software's Encase™, or PowerForensics™ as appropriate, to create a timeline of the incident and identify the impact of the incident. Additionally, we will use Infocyte to scale-ably survey the surrounding network for indications of compromise to help identify the scope of the breach.

Scope of the Assessment

Duration: 30 days	**Controllers**: (1) Active
Endpoints Scanned: 776	**Agents Deployed:** 25
Surveys Completed: 15,000+	**Objects Analyzed:** 425,477
Survey Schedule: Daily	**Applications Analyzed:** 2,883

Target Groups	Device Count	Target Groups	Device Count	Target Group	Device Count
Servers – CLE	150	Servers – CIN	100	Clients – DFW	1,000
Clients – ATL	250	Clients – STL	259	DMZ	8

Threat Analysis Overview

Devices to review:	Top Concerns:
24	**OBJ-MTI1** **Type:** Malware / Trojan / PowerShell Script Memory Injection **Names**: Yellow Cockatoo | Jupyter InfoStealer **Infocyte Score:** 10 | **Threat Score:** Undetected by standard means. **Host:** hostname1.Domain.int
Confirmed Malicious: 2 on 2 devices Threats Found (Bad): 5 on 5 devices Objects to review: 7 on 5 devices Controlled Items: 12 on 594 devices Unwanted Objects: 16 on 14 devices	**OBJ-MTD2** **Type:** Malware / Trojan **Name:** caldwell-county-texas-sample-ballot.exe **Infocyte Score:** 10 | Threat Score: 33 of 66 **Host:** hostname2.Domain.int

	OBJ-HA1 **Type:** Hack tool / Adware / Win32/KMSAuto!MSR **Name**: office 2010 activation and conversion kit 1.6.exe **Infocyte Score:** 7 | Threat Score: 46 of 67 **Host:** hostname3.Domain.int

Vulnerability Analysis Overview

Vulnerabilities CVSS v3 > 9:	Top Vulnerability Concerns:
3 **Critical Vulnerabilities Found:** 2 (CVSS v3 greater than 9, with more than 50 advisories) Note: General Browser Vulnerabilities are not included as Critical	iTunes from Apple Software CVSS v3 Score: 9.8 Advisories: 378 Versions Found: 12.10.6.2, 12.10.1.4, 12.9.4.102, 12.10.7.3, 12.10.4.2
	iCloud from Apple Software CVSS v3 Score: 9.8 Advisories: 203 Versions Found: 7.21.0.23, 7.4.0.111
	VLC Media Player from VideoLAN CVSS v3 Score: 9.8 Advisories: 49 Versions Found: 2.2.2, 2.2.4, 2.2.6

Critical Threat Analysis

Legend

Trojan		Ransomware	
Data Theft		Hack Tool	
File Dropper		Adware / Unwanted	

OBJ-MTI1	cli-40910ba08f7b27def843e078851dd554a9b40b48	**Score** 10	**Confidence** 99%	
First Found:	January 25, 2021	Last Found:	February 12, 2021	
Name(s):	Jupyter InfoStealer, Yellow Cockatoo	MD5 Hash:	157569cb7b603e45b6f4a66327ddee0a	
Description:	Jupyter InfoStealer is a name given to the threat group and their custom trojan designed to gather and exfiltrate private and sensitive (i.e. PII) information from a target system. First observed in second half of 2020, this malware has demonstrated highly targeted attacks using lightweight and stealthy malware that often do not propagate or persist in a network (get-in and get-out tactics). This type of trojan is particularly difficult to detect as it leaves an extremely small footprint. Observed entry vectors range from web browser exploitation to spear phishing via email.			
TTP(s):	Delivery: PowerShell Script, fileless malware injection into volatile memory. Persistence: URL Link in Start-Up folder.			
Devices:	Hostname1.domain.int, no other detections	Username(s):		
File path(s):	Script: c:\users\<<username>>\appdata\roaming\microsoft\yetj\jnpnxycw.cmd Persistence:\microsoft\windows\start menu\programs\startup\add375f568547c9bc8c38d92878f1.lnk			
Remediation:	Option 1: Replace machine and / or low-level format and reimage. Change all passwords for affected user(s). Option 2: Attempt remediation by removing the script located at the path above. Remove the Persistence Mechanism. Change all passwords for the affected user(s). Rescan with Infocyte daily to confirm the compromise does not return.			
Actions:	Threat was disclosed to <<Company Name>> via conference call. The <<Company Name>> team will be remediating this compromise by replacing the user's machine, and changing the passwords utilized on this machine.			

OBJ-MTD2	caldwell-county-texas-sample-ballot.exe	Score 10	Confidence 99%	
First Found:	January 25, 2021	Last Found:	January 25, 2021	
Name(s):	MSIL/Gorf, POLAZERT.WLB	MD5 Hash:	7be0725643c89e332b0434536a96de50	
TTP(s):	Delivery: Executable utilizes PowerShell to add commands to conhost.exe to run as a fileless malware. Persistence: Autostart link created by PowerShell launched at runtime.			
Devices:	Hostname2.domain.int, no other detections	Username(s):		
File path(s):	Executable: c:\users\<username>\downloads\caldwell-county-texas-sample-ballot.exe Persistence: AutoStart link created by PowerShell launched at runtime. Files Written: Reference VirusTotal			
Remediation:	Option 1: Replace machine and / or low-level format and reimage. Change all passwords for affected user(s). Option 2: Attempt remediation by removing the script located at the path above. Remove the Persistence Mechanism. Change all passwords for the affected user(s). Rescan with Infocyte daily to confirm the compromise does not return.			
Actions:	Threat was disclosed to <<Company Name>> via conference call. The <<Company Name>> team will be remediating this compromise by replacing the user's machine, and changing the passwords utilized on this machine.			

OBJ-HA1	office 2010 activation and conversion kit 1.6.exe	Score 5	Confidence 99%	
First Found:	February 12, 2021	Last Found:	February 12, 2021	
Name(s):	KMSausto, KMSActivator	MD5 Hash:	c07c80efd4a65b4ef8a9ce01a7183c36	
TTP(s):	Delivery: Executable Persistence: Installed			
Devices:	Hostname3.domain.int, no other detections	Username(s):	NA	
File path(s):	Executable: d:\pictures\pix\misc\office 2010 activation and conversion kit 1.6.exe Persistence: Installed application Files Written: Reference VirusTotal			
Remediation:	Option 1: This application can be uninstalled via normal means. This application is not inherently malicious but is considered a Hack Tool that can allow users to generate licenses, or brute force license registration.			
Actions:	Threat was disclosed to <<Company Name>> via conference call. The <<Company Name>> Team will remove the application.			

Software Vulnerabilities

This threat assessment includes an assessment of the software vulnerabilities found in the environment in installed applications. The scoring system is based on the overall exploitability (CVSS v3 score) and the total number of advisories found for the installed applications. The referenced information is publicly available in the National Vulnerability Database located at: https://nvd.nist.gov/vuln/

This assessment does not test if the vulnerabilities have been exploited specifically, but in accordance with the charter of this Threat Assessment, malicious code, and exploits would be found through the advanced threat hunting capabilities of the Infocyte Endpoint Protection platform.

Inside <<Company Name>>'s infrastructure, two applications rose to the level of critical vulnerabilities and have been included in the supporting documentation. Reference: Vulnerabilities Zip (7zip).GZ. These two applications, iCloud and iTunes, are likely not needed in a business setting, and may be further addressed with policy changes.

The most effective way to address the vulnerabilities found in this assessment is to remove unwanted or unnecessary applications and maintain updates on the applications that will remain.

A note about Web Applications: *Internet browsers and Internet tools, will remain an ever-changing threat due to the need to maintain backwards capabilities—ensuring the user experience on older web portals is not impacted. It is best to standardize on specific tools and keep them at the latest available version.*

Recommendations and Conclusion

The following recommendations should be considered for ongoing operations at <<Company Name>>. Please note that the SOC analysts at Infocyte are not aware of all policies and procedures that may already be in place. These recommendations are made based solely on the assessed environment, and the information found.

Recommendation 1 – Restrict Permissions

Allowing users to download and execute applications from any location on the internet, or items received via email, can expose <<Company Name>> to undue risk. Consider restricting administrative privileges and/or application execution controls on end user devices where applicable. This change would have likely prevented the installation of OBJMTD2, and the unwanted / adware applications found during the assessment.

Conclusion

The majority of the <<Company Name>> infrastructure was relatively secure, however, two objects found represent a high level of exposure for potential data loss. These two threats were localized on two machines, no attempts to expand beyond these machines were found by the Infocyte SOC. Instead, both malicious applications appear to be focused on the information contained on said machines. Due to the nature of these threats, Infocyte recommends retaining a licensed digital forensics firm to investigate the root cause and impact of the attack.

The remaining objects, potentially unwanted applications, administrative tools, and adware represent a low level of potential risk. These secondary objects could further expose the environment to unknown exploitable vulnerabilities and should be addressed as time allows.

Appendix

Supporting Documentation:

Report Name	File Name	Description
Threat Report by Host	Threats by Host.PDF	Threats Found by Host
Threat Report by Threat	Threats by Threat.PDF	Threats Found by Threat
Asset Report Hardware	Device_List_Final.CSV	A list of hardware found
Asset Report Software	Software Asset Report.PDF	A list of software found
Vulnerabilities Report	Vulnerabilities Zip (7zip).gz	GZ zipped CSV of Vulnerabilities
Controlled Items	Controlled_Items_Final.CSV	List of Controlled Items
Extensions (Sunburst)	Extensions_Ran_Result.csv	Results from SolarWinds Analysis
Installed Agents	Installed_Agents.csv	List of agents installed
Objects for review	Objects_For_Review.csv	Items to review
Probably Good Items	Probably_Good_Items_Final.csv	List of items deemed good.
Target Group Report	TargetGroupList.csv	Target Groups and Devices
Unwanted Applications	Unwanted_Applications_Final.csv	List of unwanted applications
Verified Bad Items	Verified_Bad_Final.csv	Items deemed “bad”