KEYSIGHT TECHNOLOGIES

Breach Defense

Threat Simulator 1.0.1 – SaaS Infrastructure

Threat Simulator 1.0.3 – ATI 2020-06-15

Release Notes 15th June 2020

Deployment Version:	1.0.2.1903
AAM Cluster Version:	1.0.2.1897
Recommended Agent Version	2.3.25-1586815322
ATI Live JIT:	20.6.38.388356
ATI Recommendations DB:	20.6.1143.388302
ATI Version:	20.6.1065.387084

Notices Copyright Notice ©

Keysight Technologies 2005 – 2020

No part of this document may be reproduced in any form or by any means (including electronic storage and retrieval or translation into a foreign language) without prior agreement and written consent from Keysight Technologies, Inc. as governed by United States and international copyright laws.

Warranty

The material contained in this document is provided “as is,” and is subject to being changed, without notice, in future editions. Further, to the maximum extent permitted by applicable law, Keysight disclaims all warranties, either express or implied, with regard to this manual and any information contained herein, including but not limited to the implied warranties of merchantability and fitness for a particular purpose. Keysight shall not be liable for errors or for incidental or consequential damages in connection with the furnishing, use, or performance of this document or of any information contained herein. Should Keysight and the user have a separate written agreement with warranty terms covering the material in this document that conflict with these terms, the warranty terms in the separate agreement shall control.

Technology Licenses

The hardware and/or software described in this document are furnished under a license and may be used or copied only in accordance with the terms of such license.

U.S. Government Rights

The Software is "commercial computer software," as defined by Federal Acquisition Regulation ("FAR") 2.101. Pursuant to FAR 12.212 and 27.405-3 and Department of Defense FAR Supplement ("DFARS") 227.7202, the U.S. government acquires commercial computer software under the same terms by which the software is customarily provided to the public. Accordingly, Keysight provides the Software to U.S. government customers under its standard commercial license, which is embodied in its End User License Agreement (EULA), a copy of which can be found at http://www.keysight.com/find/sweula or https://support.ixiacom.com/supportservices/warranty-license-agreements. The license set forth in the EULA represents the exclusive authority by which the U.S. government may use, modify, distribute, or disclose the Software. The EULA and the license set forth therein, does not require or permit, among other things, that Keysight: (1) Furnish technical information related to commercial computer software or commercial computer software documentation that is not customarily provided to the public; or (2) Relinquish to, or otherwise provide, the government rights in excess of these rights customarily provided to the public to use, modify, reproduce, release, perform, display, or disclose commercial computer software or commercial computer software documentation. No additional government requirements beyond those set forth in the EULA shall apply, except to the extent that those terms, rights, or licenses are explicitly required from all providers of commercial computer software pursuant to the FAR and the DFARS and are set forth specifically in writing elsewhere in the EULA. Key-sight shall be under no obligation to update, revise or otherwise modify the Software. With respect to any technical data as defined by FAR 2.101, pursuant to FAR 12.211 and 27.404.2 and DFARS 227.7102, the U.S. government acquires no greater than Limited Rights as defined in FAR 27.401 or DFAR 227.7103-5 (c), as applicable in any technical data. 52.227-14 (June 1987) or DFAR 252.227-7015 (b)(2) (November 1995), as applicable in any technical data.

Threat Simulator 1.0.1 – SaaS Infrastructure

Document Scope

This document provides information regarding the Threat Simulator 1.0.1, including information about new features, resolved SRs, known defects and workarounds.

Browser Compatibility

Threat Simulator 1.0.1 is compatible with the following browsers

- Google Chrome browser 81.0.4044.92
- Firefox browser 75.0

Browser versions that are more current than the versions listed in the table may work but have not been tested at this time.

New Features in Release 1.0.1

REST API Support I

- A REST API is available to allow a configured scenario to be run and the results retrieved.
- Access to the REST feature is available under “Settings”.
- The API is self-documenting, a user can use an API token to test calls from the UI

Agent Installer

- Improved Error handling and Logging
- New installer option for silent installation (-y)
- New uninstall option to delete containers (-d)

Agent OVA

- An OVA is available, allowing a user to quickly set up a virtual environment for a Threat Simulator Agent
- User can install the OVA and use the “Deployment > On Premises” tutorial to install an Agent

Issues Addressed in 1.0.1

- THREATSIM-10724 Addressed random audits blocked running against AWS LB
- THREATSIM-10671 Stops SIEM events older than 3 days are being deleted
- THREATSIM-10602 Ensures Dashboard shows the latest history by default
- THREATSIM-10600 Fixes Dashboard Assessment History incorrectly reported results
- THREATSIM-10599 Prevents Agent being added to Topology if install fails
- THREATSIM-10565 Enhancement to warn users if they create a duplicate custom tag
- THREATSIM-10480 Improves Agent installer ping reliability
- THREATSIM-10417 Prevents Trial Mode banner from overlapping SIEM window
- THREATSIM-10363 Adds a spinner while Agent tags are deleted.
- THREATSIM-10347 Fixes assessment run getting stuck in Queued state
- THREATSIM-10282 Adds indication that Path Discovery Rescan is active
- THREATSIM-10268 Fixes Inconsistent status between Topology and Agent Pages
- THREATSIM-10240 Corrects the link for agent download by adding "-api"
- THREATSIM-10196 Improves reliability of Agents table reboot function
- THREATSIM-10195 Addresses browser refresh for Topology update triangle
- THREATSIM-10145 Addresses browser refresh for available licenses
- THREATSIM-10137 Fixes HTTP failure response when activating license
- THREATSIM-9704 Allows user to create killchain scenarios with different configurations
- THREATSIM-9629 Enables Agent CloudFormation support in AWS eu-west-3 region
- THREATSIM-8776 Allows Path discovery to be triggered again if it has fails

Limitations and Known Issues

THREATSIM-10840 Docker restarting-loop on Ubuntu 18.04 / 20.04 LTS Desktop/Server

- On Ubuntu-based hosts running 18.04 LTS/20.04 LTS (and probably 16.04 LTS), a fresh Threat Simulator agent installation fails to bring the docker containers up, even though the installation completes without errors. As a result, the agent will show offline in the user interface. The docker container logs command will indicate Permission Denied.This is due to a change that the latest snap docker version has some collateral that seems to be widespread and affects many users on internet.
- If you need to deploy a new Threat Simulator agent on Ubuntu, please pre-install docker container using sudo apt install docker.io command. This docker installation method doesn't have the bug and allows our agent to run properly after install
- For systems where the snap docker version was installed by a prior attempt to deploy our agent, you can correct the issue using the following commands:
    - kill and remove all containers, then remove all container images on host
        - sudo docker kill $(sudo docker ps -a -q)
        - sudo docker container rm $(sudo docker ps -a -q)
        - sudo docker image rmi $(sudo docker images -q)
    - Remove snap docker
        - sudo snap docker remove

    - install docker.io version
        - sudo apt install docker.io
    - Re-install our agent using standard procedure

THREATSIM-10287: Threat Simulator agent supports only IPv4 addresses

- When deploying a Threat Simulator agent on a Linux host with IPv6 address enabled the install may fail. To work around this issue, disable IPv6 and rerun the install script

THREATSIM-10288 Docker Snap may interfere with Agent Installation

- When deploying Threat Simulator on a supported Linux-host that has Docker Snap installed, Docker Snap may conflict with the Docker.io installed by Threat Simulator. To work around this issue, remove Docker Snap and rerun the install script

THREATSIM-10289 UI Response “Serverless Cold Start”

- When unused the services that support the UI are shut down. After logging in the first access to a page in the application may be slow to load time. Subsequent accesses should not experience this lag.

THREATSIM-10290 Assessment complete with Error

- On rare occasions an assessment may complete with an Error. This can be caused by a variety of reasons such as loss of communication with the agent while the assessment is running. If an Assessment Completes with an error, the results of that run will not count in the aggregated results (Health Score), the last successful run will be used. If an error occurred, the user can rerun the Assessment. In future updates we will consider adding the option to automatically rerun on error.

THREATSIM-0385 Audit Reports False Positive (Blocked)

- On rare occasions an Audit may be reported with a false “Pass – Blocked”. This can be caused by a variety of reasons such as loss of communication with the agent while the assessment is running. Typically, there are hundreds of Audits run on a path and a single false positive has little impact on the overall (Health Score).

Operational Notes

THREATSIM-10203 Assessment will run when "Access Control" blocks traffic

- An assessment will run on path regardless of access controls. For example, by default, Web Browser Assessment uses HTTPS: 443. If the network blocks all HTTPS: 443 traffic, the assessment will still run, each audit will report “PASS, BLOCKED, Access Blocked on HTTPS: 443.

THREATSIM-10253 Secondary Management Interface may be Required on Agent

- To operate, a Threat Simulator Agent needs to communicate to the Threat Simulator Manager. This requires the following rules:
  - Outbound, HTTPS: 443, with tar.gz file download
  - Outbound MQTT: 8883
- If required, an Agent can be deployed with a separate interface for "Management Traffic and “Test Traffic”. Refer to "Deployment Tutorials" for more information

THREATSIM-9791 Agent errors with timeout when port 10000 is already in use on the host machine

- When deploying Threat Simulator on a supported Linux-host that has port 10000 already in use, the audits complete with a timeout Error. To work around this issue, stop or remove the application that uses port 10000.

Threat Simulator 1.0.3, ATI 2020-06-15

Document Scope

This document provides information regarding the Threat Simulator 1.0.3, including information about new features, resolved SRs, known defects and workarounds (if available). This is a comprehensive document combining all previous release details into one.

For reference previous updates are also included.

Release Overview

This release is an incremental Threat Intelligence content update.

Key Highlights

- 6 new audits
- 2 new security assessments

For a complete listing of all the new features included in this release, please refer to the '*What is New*' section

What is New

New Assessments (2)

Assessment Name	Category	Info
CISA Top 10, 2016-2019 Server Attacks	Instrumentation	On May 12, 2020 the Cybersecurity and Infrastructure Security Agency (CISA) published Alert AA20-133A: Top 10 Routinely Exploited Vulnerabilities. Based on technical analysis by the Federal Bureau of Investigation (FBI), and U.S. Government reporting, the compiled list identifies the vulnerabilities most frequently exploited by state, nonstate, and unattributed cyber actors from 2016 to 2019. https://www.us-cert.gov/sites/default/files/publications/AA20-133A_Top_10_Routinely_Exploited_Vulnerabilities_S508C.pdf The vulnerabilities in the CISA Top 10 2016-2019 list satisfy a combination of typical criteria exploited by attackers: the affected applications are widely deployed, exploits for the vulnerabilities are generally available, the vulnerability enables an attacker to execute malicious code and the attacker can easily reach, directly or indirectly, a target system. This assessment contains audits targeting vulnerabilities in applications typically found running on server systems. * CVE-2019-0604 - Microsoft Sharepoint Insecure Deserialization * CVE-2018-7600 - Drupal CMS Insecure PHP Deserialization * CVE-2017-5638 - Apache Struts2 OGNL OS Command Injection The audits in this assessment are classified as direct attacks, meaning they can be exploited by an attacker without requiring any interaction with the victim. These attacks can be especially damaging to an organization as the targeted applications are frequently deployed on internet-facing hosts, significantly increasing the scope of potential attackers. This assessment will run through each of the audits one-by-one in order to test how well your implemented security controls protect your servers against these attacks. * If an audit results in Pass, this indicates one of the tested security controls prevented the attack. * If an audit results in Failure, this indicates that all tested security controls failed to prevent the attack.
CISA Top 10, 2016-2019 Client Attacks	Instrumentation	On May 12, 2020 the Cybersecurity and Infrastructure Security Agency (CISA) published Alert AA20-133A: Top 10 Routinely Exploited Vulnerabilities. Based on technical analysis by the Federal Bureau of Investigation (FBI), and U.S. Government reporting, the compiled list identifies the vulnerabilities most frequently exploited by state, nonstate, and unattributed cyber actors from 2016 to 2019. https://www.us-cert.gov/sites/default/files/publications/AA20-133A_Top_10_Routinely_Exploited_Vulnerabilities_S508C.pdf The vulnerabilities in the CISA Top 10 2016-2019 list

		satisfy a combination of typical criteria exploited by attackers: the affected applications are widely deployed, exploits for the vulnerabilities are generally available, the vulnerability enables an attacker to execute malicious code and the attacker can easily reach, directly or indirectly, a target system. This assessment contains audits targeting vulnerabilities in applications typically found running on client systems. * CVE-2012-0158 Microsoft Windows Common Controls MSCOMCTL.OCX Stack Overflow * CVE-2015-1641 Microsoft Office Word Memory Corruption Vulnerability * CVE-2017-11882 Microsoft Office EQNEDT32.exe Font Name Stack Buffer Overflow * CVE-2017-0199 Microsoft Office/Wordpad Remote Code Execution via URL Moniker * CVE-2017-8759 Microsoft .Net Framework WsdlParser Remote Code Execution * CVE-2018-4878 Adobe Flash Player DRMManager Use After Free The audits in this assessment are classified as indirect attacks, meaning they require some interaction with the victim in order to exploit the vulnerability. The exploits used in these attacks are file-based, requiring the victim to use the vulnerable application to interact with the malicious file. Attackers user various techniques such as phishing, drive-by-downloads, 'free' flash-drives in order to ensure the vulnerable application is used to interact with the malicious file. These attacks can be especially damaging to an organization due to the number of potential victims, significantly increasing the scope of the attack surface. This assessment will run through each of the audits one-by-one in order to test how well your implemented security controls protect your clients against these attacks. * If an audit results in Pass, this indicates one of the tested security controls prevented the attack. * If an audit results in Failure, this indicates that all tested security controls failed to prevent the attack.

New Audits (6)

Assessment Name: CISA Top 10, 2016-2019 Server Attacks

Audit Name	MITRE ATT&CK	CVE	References
Microsoft SharePoint 'DecodeEntityInstanceId' Insecure Deserialization	T1190	2019-0604	This audit exploits an insecure deserialization vulnerability in Microsoft SharePoint. The vulnerability is due to insufficient validation of user-supplied data to 'EntityInstanceIdEncoder' class. A remote, authenticated attacker could exploit this vulnerability by sending maliciously crafted HTTP requests to a

			target SharePoint server. Successful exploitation of this vulnerability leads to remote code execution on the target SharePoint web application.
Grandstream UCM6202 Remote SQL Injection	T1190	2020-5722	Grandstream UCM6200 series is vulnerable to an unauthenticated remote SQL injection via a crafted HTTP request. A remote attacker can use this vulnerability to either execute shell commands under root privileges (on versions before 1.0.19.20) or inject HTML in password recovery emails (on versions before 1.0.20.17).

Assessment Name: CISA Top 10, 2016-2019 Client Attacks

Audit Name	MITRE ATT&CK	CVE	References
Microsoft Windows Common Controls MSCOMCTL.OCX Stack Overflow	T1189	2012-0158	This audit exploits a stack buffer overflow vulnerability that exists in the Microsoft Windows Common Controls module (MSCOMCTL.OCX). The vulnerability is due to improper handling of objects in memory. The vulnerability can be exploited by crafting a malicious DOC file and enticing a user to download and open it. Successful exploitation may result in execution of arbitrary code with the privileges of the application using the vulnerable module.
Microsoft .Net Framework WsdlParser Remote Code Execution	T1189	2017-8759	This audit exploits a Remote Code Execution vulnerability in Microsoft .Net Framework. The vulnerability is due to improper validation of user-controlled input while parsing WSDL files. An attacker could remotely execute arbitrary code on a target system by convincing a target user to open a malicious document.
Google Chrome 'kJSCreate' Type Confusion Code Execution	T1189	2020-6418	A type confusion vulnerability exists in V8 JavaScript engine in Google Chrome prior to 80.0.3987.122. The vulnerability may be triggered by changing array elements types (e.g. from SmallInteger to Double) after optimization takes place. By successfully exploiting this flaw, an attacker can execute arbitrary code in the context of the Chrome's 'renderer' process.
Adobe Flash Player DRMManager Use After Free	T1189	2018-4878	This audit exploits a remote code execution vulnerability in Adobe Flash Player. The vulnerability is due to a Use-After-Free found in vulnerable methods inside object DRMManager. An attacker can entice a target to open a specially crafted Flash file to trigger the vulnerability. Successful exploitation may result in execution of arbitrary code or abnormal termination of the Flash plugin.

Release 1.0.2 (2020-05-31)

New Kill Chain Assessments (2)

Assessment Name	Category	Info
Word Doc with DNS Tunneling	Kill Chain	This assessment showcases two common evasion-techniques used by malware authors: multi-layered payload-obfuscation and covert data-smuggling.
Word Doc with HTTP Exfiltration	Kill Chain	This assessment showcases two common evasion-techniques used by malware authors: multi-layered payload-obfuscation and covert data-exfiltration.

New Audits (21)

Assessment Name: Word Doc with DNS Tunneling (Category: Kill Chain)

Audit Name	MITRE ATT&CK	References
Word Macro DNS Tunneling 'Macro-decoded PowerShell MalDoc' File transfer	T1189	This audit simulates the network transfer of Word Macro DNS Tunneling 'Macro-decoded PowerShell MalDoc' module.
Word Macro DNS tunneling Command and Control	T1148	This audit simulates Word Macro DNS Command and Control traffic after executing 'Macro-decoded PowerShell MalDoc'.

Assessment Name: Word Doc with HTTP Exfiltration (Category: Kill Chain)

Audit Name	MITRE ATT&CK	References
Macro-Enabled Word Document File transfer	T1189	This audit simulates the network transfer of a Macro-Enabled Word Document.

Microsoft Media Foundation 'IMFASFSplitter::Initialize' Type Confusion	T1022	This audit exfiltrates host information via HTTP POST request.

Assessment Name: Media File Vulnerabilities (Category: Instrumentation)

Audit Name	MITRE ATT&CK	References
Microsoft Adobe Font Manager Library Type 1 BlendDesignPositions Handling Buffer Overflow	T1189	A memory corruption vulnerability has been reported in Adobe Type Manager component of Microsoft Windows. The vulnerability is due to improper handling of specially crafted BlendDesignPositions array in multiple master Type 1 fonts. A remote attacker can exploit this vulnerability by enticing a user to open a specially crafted font file. Successful exploitation could result either in the execution of arbitrary code with SYSTEM or UMFD permissions or denial of service condition.
Microsoft Media Foundation GetKeyForIndex Out-of-Bounds Read	T1189	An information disclosure vulnerability has been reported in the Windows Media Foundation component of Microsoft Windows. The vulnerability is due to improper handling of objects in memory. A remote attacker can exploit this vulnerability by enticing a user to open a specially crafted QuickTime media file. Successful exploitation could result in the execution of arbitrary code within the context of the user running the application.

Assessment Name: PDF Document Vulnerabilities (Category: Instrumentation)

Audit Name	MITRE ATT&CK	References
Adobe Reader Acroform UTF-16 BOM Field Use After Free	T1189	A use after free vulnerability exists in Adobe Reader and Acrobat due to incorrect manipulation of objects in memory. The vulnerability exists in 'AcroForm.api' dynamic library and may be triggered by a Field object that begins with an UTF-16 BE BOM sequence. An attacker may execute arbitrary code on a victim's system by enticing the victim to open a crafted PDF file.

Assessment Name: Office Document Vulnerabilities (Category: Instrumentation)

Audit Name	MITRE ATT&CK	References
Microsoft Office EQNEDT32.exe Font Name Stack Buffer Overflow	T1189	This audit exploits a buffer overflow vulnerability in EQNEDT component of Microsoft Office. The vulnerability is due to an invalidation of font name field length in an OLE object. An attacker could execute arbitrary code by enticing a user to open a maliciously crafted document using the vulnerable software.

Assessment Name: Web Browser Firefox (Category: Instrumentation)

Audit Name	MITRE ATT&CK	References
Mozilla Firefox ReadableStreamCloseInternal Out of Bounds Access	T1189	This audit exploits a vulnerability in Spidermonkey, the Javascript engine of Mozilla Firefox. An attacker can craft Javascript promise resolutions in such a way that make it possible to cause an out-of-bounds read off the end of an array resized during script execution. This can lead to a denial of service or potentially allow for remote code execution to occur.

Assessment Name: Web Browser Miscellaneous (Category: Instrumentation)

Audit Name	MITRE ATT&CK	References
Oracle iPlanet Admin Panel Image Injection	T1189	An image injection vulnerability exists in Oracle iPlanet Web Server versions 7.0.x, due to poor 'productNameSrc' HTTP parameter sanitization. By tricking an admin to follow a crafted URL, a remote attacker may perform phishing attacks by injecting a custom image in the admin panel.

Assessment Name: Malware File Transfer (Category: Instrumentation)

Audit Name	MITRE ATT&CK	Audit Name
Malware: Maze Ransomware variant 1	T1189	Maze ransomware is a malicious program that encrypts files of the victim and demands a ransom in exchange for a decryption key that restores information. After execution, the Maze deletes shadow copies and encrypts all targeted files. Finally, the Maze drops a ransom note on the desktop.
Malware: Maze Ransomware variant 2	T1189	Maze ransomware is a malicious program that encrypts files of the victim and demands a ransom in exchange for a decryption key that restores information. After execution, the Maze deletes shadow copies and encrypts all targeted files. Finally, the Maze drops a ransom note on the desktop.
Malware: Maze Ransomware variant 3	T1189	Maze ransomware is a malicious program that encrypts files of the victim and demands a ransom in exchange for a decryption key that restores information. After execution, the Maze deletes shadow copies and encrypts all targeted files. Finally, the Maze drops a ransom note on the desktop.
Malware: Maze Ransomware variant 4	T1189	Maze ransomware is a malicious program that encrypts files of the victim and demands a ransom in exchange for a decryption key that restores information. After execution, the Maze deletes shadow copies and encrypts all targeted files. Finally, the Maze drops a ransom note on the desktop.

Assessment Name: Web Application Security (Category: Instrumentation)

Audit Name	MITRE ATT&CK	References
ZyXEL NAS 'weblogin.cgi' OS Command Injection	T1190	An OS command injection vulnerability exists in multiple ZyXEL products due to insufficient user input sanitization when parsing the 'username' parameter. By sending a crafted HTTP request, a remote unauthenticated attacker may execute arbitrary OS commands as a superuser.
ThinkPHP Remote Code Execution	T1190	This audit exploits a remote code execution in ThinkPHP framework. The flaw is rooted within the 'invokefunction' method as a consequence of no parameter validation. A remote, unauthenticated attacker may thus be able to execute code on the vulnerable machine with the permissions of the user running the web server.
Jenkins Remote Code Execution	T1190	This audit exploits a remote code execution vulnerability in Jenkins. The vulnerability is due to improper filtering of the "value" parameter when invoking a method on Java objects. An attacker could exploit this vulnerability by sending a crafted HTTP request to the target server. Successful exploitation results in remote code execution on the target server.
Drupal Core PHP Deserialization Remote Code Execution	T1190	This audit exploits a vulnerability in Drupal Core open-source CMS. The vulnerability is due to improper validation of user-supplied data while performing server-side deserialization of PHP objects. A malicious user can exploit this vulnerability by sending multiple HTTP POST requests including serialized PHP objects. When successfully exploited, the vulnerability results in complete compromise of the target server.
Oracle iPlanet Web Server Information Disclosure	T1190	An information disclosure vulnerability exists in Oracle iPlanet Web Server versions 7.x and prior. By accessing specific paths related to the admin panel, a remote unauthenticated attacker may obtain sensitive information regarding server's configuration.

Assessment Name: Remote Access (Category: Instrumentation)

Audit Name	MITRE ATT&CK	References
Citrix Application Delivery Controller Command Injection via 'vpn' Directory Traversal	T1190	An OS command injection vulnerability exists in Citrix Application Delivery Controller (ADC) and Gateway 10.5, 11.1, 12.0, 12.1, and 13.0. The command injection is possible using a directory traversal flaw, due to improper sanitization of multiple fields in HTTP requests. The flaw may be exploited by an unauthenticated attacker to execute arbitrary commands on the target server.

Assessment Name: Web Application OS Command Injection (Category: Instrumentation)

Audit Name	MITRE ATT&CK	References
Nexus Repository Manager 3 Remote Code Execution	T1190	This audit exploits a remote code execution on Nexus Repository Manager 3. This vulnerability is due to improper handling of the "value" parameter under HTTP parameter when a client sends http traffic to the server. A remote unauthenticated attacker can exploit this vulnerability by sending crafted http requests to the target server. Successful exploitation results in remote code execution.

Release 1.0.1 (2020-05-16)

New Kill Chain Assessments (2)

Assessment Name	Category	Info
Hancitor Covid19 Malspam	Kill Chain	Hancitor Covid19 Mailspam is a KillChain Assessment simulating a phishing email with a link leading to download of Hancitor malware.
WannaCry Infection and Spread - Internal Source	Kill Chain	WannaCry Infection and Spread – Internal source simulates the behavior of an internal host on the local network attempting to spread WannaCry ransomware laterally.

New Instrumentation Assessments (1)

Assessment Name	Category	Info
Remote Access	Instrumentation	A collection of audits targeting vulnerabilities in applications providing remote access to internet-connected clients.

New Audits (10)

Assessment Name: Hancitor COVID-19 Mailspam (Category: Kill chain)

Audit Name	MITRE ATT&CK	References
Hancitor Malware April 2020 Campaign 'VBS' File transfer"	T1189	https://www.hybrid-analysis.com/sample/0caef27... MD5: 0573214d694922449342c48810dabb5a SHA1: f14538d59be374fa17d10ef762ec9db3344d2c20 SHA256: 0caef2718bc7130314b7f08559beba53ccf00e5ee5aba49523fb8 This audit simulates the network transfer of the VBScript module used in Hancitor Malware April 2020 Campaign. After being downloaded the VBScript module executes PowerShell commands in order to gather host-related information prior to exfiltration to the Command and Control server.
COVID-19 Phishing Email	T1192	This audit simulates a phishing email that was distributed in-the-wild in March of 2020. The phishing email purports to being from a well-known insurer (Cigna) with timely content: Update to insurance coverage related to Coronavirus (also known as COVID-19). Within the html-based email is a link that the user is supposed to click in order to see updated billing information. However, if the link is clicked, it will instead initiate an HTTP request to a malware server, which instead serves Hancitor malware. Interesting Notes: • The email headers suggest the originating SMTP server was Russian: smtp16.mail.ru (mail.ru is a popular Russian web-based email service). • There are 2 'mistakes' which may be an attempt to evade security-device payload-inspection or merely an error on part of attacker • The email header 'Content-Type: multipart/alternatve; boundary="_417_82207006"' has an incorrect type (should be 'multipart/alternative') • The html header 'ContentType: text/plain; charset="windows-1251"' is invalid (should be 'Content-Type:').

Assessment Name: LAN Perimeter Security > File Vulnerability > Media (Category: Instrumentation)

Audit Name	MITRE ATT&CK	References
Microsoft Media Foundation CMP4MetadataHandler AddQTMetadata Use After Free	T1189	CVE-2019-1430 https://talosintelligence.com/vulnerability_reports/TALOS-2019-0946 CVSSv3: 7.8 (CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H) A memory corruption vulnerability has been reported in Windows Media Foundation component of Microsoft Windows. The vulnerability is due to improper handling of objects in memory. A remote attacker can exploit this vulnerability by enticing a user to open a specially crafted QuickTime media file. Successful exploitation could result in the execution of arbitrary code within the context of the user running the application.
Microsoft Media Foundation 'IMFASFSplitter::Initialize' Type Confusion	T1189	CVE-2020-0738 CVSSv3: 8.8 (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H) https://talosintelligence.com/vulnerability_reports/TALOS-2019-0946 A memory corruption vulnerability has been reported in Windows Media Foundation component of Microsoft Windows. The vulnerability is due to improper handling of objects in memory. A remote attacker can exploit this vulnerability by enticing a user to open a specially crafted ASF media file. Successful exploitation could result in the execution of arbitrary code within the context of the user running the application.

Assessment Name: Remote Access (Category: Instrumentation)

Audit Name	MITRE ATT&CK	References
Cisco Adaptive Security Appliance - Path Traversal	T1190	CVE-2018-0296 CVSSv3: 7.5 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H) https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20180606-as This audit exploits a vulnerability of the Cisco Adaptive Security Appliance (ASA) web interface. The vulnerability is due to improper input validation of the HTTP URL. An attacker could exploit this vulnerability by sending a specially crafted HTTP request to the target device. A successful exploit could allow the attacker to cause a DoS condition or unauthenticated disclosure of information.
Pulse Connect Secure 'html5acc' Arbitrary File Disclosure	T1190	CVE-2019-11510 CVSSv3: 10.0 (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H) http://packetstormsecurity.com/files/154176/Pulse-Secure-SSL-VPN-8.1R15.1-8.2-8.3-9.0- This audit simulates an attack on Pulse Connect Secure versions prior to 8.1R15.1, 8.2 before 8.2R12.1, 8.3 before 8.3R7.1, and 9.0 before 9.0R3.4. The flaw takes advantage of a directory traversal vulnerability and allows remote unauthenticated attackers to read arbitrary files residing on the host system.
Microsoft Windows RDP Channel 'MS_T120' Use After Free	T1190	CVE-2019-0708 CVSSv3: 9.8 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H) https://securingtomorrow.mcafee.com/other-blogs/mcafee-labs/rdp-stands-for-really-do-patch-understanding-the-wormable-rdp-vulnerability-cve-2019-0708/ This audit replicates an attack known as Bluekeep against a Microsoft Windows RDP Server (Remote Desktop Services), exploiting a use-after-free vulnerability. The flaw resides in a single memory zone being addressed by two different pointers when creating an RDP channel with the name 'MS_T120', when the connection is set up. A successful exploitation grants the attacker complete control over the target system.

Assessment Name: Malware File Transfer (Category: Instrumentation)

Audit Name	MITRE ATT&CK	Audit Name
Malware: Ragnar Locker variant 1	T1189	Ragnar Locker is a ransomware that encrypts infected systems and demands a bitcoin ransom in order to decrypt the data. It infects these systems through unsecured RDP connections, and then uses MSP tools to push PowerShell scripts to all available endpoints. It finally uses these scripts to download a payload from Pastebin, that will execute the ransomware sample that is seen in this assessment.
Malware: Ragnar Locker variant 2	T1189	Ragnar Locker is a ransomware that encrypts infected systems and demands a bitcoin ransom in order to decrypt the data. It infects these systems through unsecured RDP connections, and then uses MSP tools to push PowerShell scripts to all available endpoints. It finally uses these scripts to download a payload from Pastebin, that will execute the ransomware sample that is seen in this assessment.
Malware: Ragnar Locker variant 3	T1189	Ragnar Locker is a ransomware that encrypts infected systems and demands a bitcoin ransom in order to decrypt the data. It infects these systems through unsecured RDP connections, and then uses MSP tools to push PowerShell scripts to all available endpoints. It finally uses these scripts to download a payload from Pastebin, that will execute the ransomware sample that is seen in this assessment.

Technical Support

Ixia headquarters
26601 West Agoura Road
Calabasas, California 91302
+1 877 367 4942 – Toll-free North America
+1 818 871 1800 – Outside North America
+1.818.871.1805 – Fax
www.ixiacom.com/contact/info

Global Support	+1 818 595 2599	support@ixiacom.com
Regional and local support contacts:		
APAC Support	+91 80 4939 6410	support@ixiacom.com
Australia	+61-742434942	support@ixiacom.com
EMEA Support	+40 21 301 5699	support-emea@ixiacom.com
Greater China Region	+400 898 0598	support-china@ixiacom.com
Hong Kong	+852-30084465	support@ixiacom.com
India Office	+91 80 4939 6410	support-india@ixiacom.com
Japan Head Office	+81 3 5326 1980	support-japan@ixiacom.com
Korea Office	+82 2 3461 0095	support-korea@ixiacom.com
Singapore Office	+656 494 8910	support@ixiacom.com
Taiwan (local toll-free number)	00801856991	support@ixiacom.com