KEYSIGHT TECHNOLOGIES

Breach Defense

Threat Simulator 1.0.6, ATI 2020-08-03

Release Notes: August 03rd, 2020

Deployment Version:	1.0.3.1932
AAM Cluster Version:	1.0.3.1932
Recommended Agent Version	2.3.28-1591729074
ATI Live JIT	20.7.54.391048
ATI Recommendations DB	20.7.1200.391048
ATI Version	20.7.1069.389985

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.

Document Scope

This document provides information regarding the Threat Simulator 1.0.6, 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

- 194 new audits
- 3 new assessments

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

Warnings and Notes (1)

There is a known limitation for the previously-released assessments: 'CISA Top 10, 2016-2019 Server Attacks', 'Remote Access', 'Suspicious User Behavior', as well as the new 'Insecure Deserialization' Assessment. When running these Assessments, unless all of the service-ports used in the assessment are open along the path, all Audits in the Assessment will be skipped. This affects any device with port-based security controls, such as Load Balancers, Firewalls, NextGeneration Firewalls, Routers and AWS deployments.

What is New

New Assessments (3)

Assessment Name	Category	Info
Operation Wizard Opium	Kill chain	Operation WizardOpium was uncovered by Kaspersky Labs. It targets Microsoft Windows hosts. There hasn't been any success in attributing this exploitation campaign to any known threat actor. For a more detailed analysis of this operation, please visit https://securelist.com/chrome-0-day-exploit-cve-2019-13720-used-in-operation-wizardopium/94866/ The scenario in this assessment contains the following steps: 1. The attacker delivers the initial exploit, identified as CVE-2019-13720, through means of social-engineering. This exploit targets the GoogleChrome browser and takes the form of a specially-crafted HTML document containing Javascript code that, upon rendering by the target browser, leads to remote code execution. Using this exploit, the attacker gains an initial foothold in the target machine. The domain of the attacker that serves this exploit is behindcorona[.]com. 2. The attacker, now having access to the target machine, makes some checks to determine the OS version. If the host is considered to be vulnerable, it downloads an EoP (Elevation of Privileges) exploit (CVE-2019-1458) that will allow him to gain complete privileges of the system. These steps are conducted automatically. 3. At this point, the machine is completely infected. The attacker can continue with either exfiltrating sensitive information or using this station as a pivot for further attacks.
Insecure Deserialization	Instrumentation	Deserialization is the process of taking data structured for a format and rebuilding it into an object. The features of the native deserialization mechanism can be repurposed for malicious effect when operating on untrusted data. Attacks against deserializers have been found to allow denial-of-service, access control, and remote code execution attacks. This assessment contains a collection of Insecure Deserialization attacks. It will run through each of the audits one-by-one in order to test how well your implemented security controls protect your assets against these attacks. If these audits are not blocked, they could compromise your application and/or put your customers and data at risk. * 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.

Assessment Name	Category	Info
DNS Server Vulnerability	Instrumentation	This assessment validates the security controls protecting commonly-used network services. It contains a collection of attacks targeting servers that provide infrastructure-type services to network-client systems, such as DNS, DHCP or LDAP. This validation assessment contains attacks targeting Domain Name System (DNS) server applications, sourced from both public and private sources. The result of successful exploitation depends on the vulnerability being targeted, payload used by exploit and configuration of the target system, but can include: Information Disclosure, Denial-of-Service (DoS), or Remote Code Execution (RCE). * 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 intermediate security controls failed to prevent the attack.

New Audits (194)

Assessment Name: DNS Server Vulnerability

Audit Name	MITRE ATT&CK	CVE	Info
ISC BIND TSIG Validation Denial of Service	T1190	2020-8617	A denial of service vulnerability exists in BIND DNS Server versions 9.0.0-9.11.18, 9.12.0-9.12.4-P2, 9.14.0-9.14.11, 9.16.0-9.16.2-9.17.0 to 9.17.1 due to lack of MAC field size check when parsing TSIG records. A remote attacker may conduct a denial of service attack by sending a crafted DNS packet which leads to abnormal process termination due to a failed assertion.

Assessment Name: Insecure Deserialization

Audit Name	MITRE ATT&CK	CVE	Info
Zoho ManageEngine Desktop Central FileStorage getChartImage Command Injection	T1190	2020-10189	This audit exploits a Java deserialization vulnerability in the Zoho ManageEngine Desktop Central. This vulnerability is in the getChartImage function of the FileStorage class, due to lack of proper validation of user-supplied data, which results in deserialization of untrusted data. A remote unauthenticated attacker can exploit this vulnerability by sending crafted HTTP requests to the target server. Successful exploitation results in remote code execution under the context of SYSTEM/root.
Oracle Weblogic Coherence 'ReflectionExtractor' T3 Insecure	T1190	2020-2883	This audit exploits an insecure deserialization vulnerability in Oracle Coherence library, which is used in popular products such as Oracle WebLogic Server. The vulnerability lies in the 'ReflectionExtractor.class' in the Coherence REST library. The

Audit Name	MITRE ATT&CK	CVE	Info
Deserialization Code Execution			vulnerability is a result of insufficient validation of T3 requests. The server allows deserialization of classes in objects embedded with T3 protocol messages. Successful exploitation leads to remote code execution, in the context of the user running the Oracle WebLogic Service.
Oracle Weblogic Coherence 'MvelExtractor' T3 Insecure Deserialization Code Execution	T1190	2020-2884	This audit exploits an insecure deserialization vulnerability in Oracle Coherence library, which is used in popular products such as Oracle WebLogic Server. The vulnerability lies in the 'MvelExtractor.class' in the Coherence REST library. The vulnerability is a result of insufficient validation of T3 requests. The server allows deserialization of classes in objects embedded with T3 protocol messages. Successful exploitation leads to remote code execution, in the context of the user running the Oracle WebLogic Service.
Apache Tomcat 'PersistenceManager' Insecure Deserialization	T1190	2020-9484	An insecure deserialization vulnerability exists in Apache Tomcat. The vulnerability is due to insufficient validation of a cached session file before deserialization. An attacker can exploit this vulnerability by crafting a malicious HTTP request. Successful exploitation results in full control of the target server.

Assessment Name: Local File Inclusion (LFI)

Audit Name	MITRE ATT&CK	CVE	Info
Cisco Data Center Network Manager 'saveZoneInputFileToServer' Directory Traversal	T1190	2019-15980	This audit exploits a directory traversal vulnerability in Cisco Data Center Network Manager. The vulnerability is due to insufficient validation of 'filename' HTTP parameter in the 'saveZoneInputFileToServer' method. An authenticated attacker can exploit this vulnerability by sending a crafted HTTP request to the target server. Successful exploitation results in arbitrary file write, which can be used to achieve remote code execution with SYSTEM privileges.

Assessment Name: Malicious PDF Documents

Audit Name	MITRE ATT&CK	CVE	Info
Nitro PDF Nested Pages Use After Free	T1189	2020-6074	A use after free vulnerability exists in PDF parser of Nitro Pro 13.9.1.155 due to incorrect manipulation of objects in memory. An attacker may execute arbitrary code on a victim's system by enticing the victim to open a crafted PDF file. Successful exploitation may lead to remote code execution with the privileges of the user running the application.

Assessment Name: Operation Wizard Opium

Audit Name	MITRE ATT&CK	CVE	Info
Microsoft Windows Win32k Window	T1189	2019-1458	This audit exploits a vulnerability in the Windows win32k kernel driver caused by improper initialized objects in

Audit Name	MITRE ATT&CK	CVE	Info
Switching Code Execution			memory. A remote attacker could successfully exploit the vulnerability to execute arbitrary code or cause a denial of service by enticing a user to execute a PE binary file. Note: this exploit was used in the 'WizardOpium' malware operation to gain higher privileges on the infected machines.
Google Chrome WebAudio OfflineAudioContext Use After Free	T1189	2019-13720	This audit exploits a use-after-free vulnerability in the WebAudio component of Google Chrome. The vulnerability is due to incorrect handling of AudioContext objects in memory. A malicious attacker can exploit this vulnerability by creating a specially-crafted HTML page and convince the target user to access it using Chrome. Successful exploitation can potentially lead to remote code execution.

Assessment Name: Remote Access

Audit Name	MITRE ATT&CK	CVE	Info
Multiple F5 Big-IP products Directory Traversal	T1190	2020-5902	This audit exploits a directory traversal vulnerability in multiple F5 Big-IP products. The vulnerability is due to improper handling of user-supplied path in HTTP requests. A remote, unauthenticated attacker could exploit this by sending a maliciously crafted request to the server. A successful attack may result in arbitrary file read, write or remote code execution in the security context of ROOT.

Assessment Name: Web Application OS Command Injection

Audit Name	MITRE ATT&CK	CVE	Info
Axis SSI anonymous view RCE	T1190		This audit exploits a command injection vulnerability in Axis SSI camera. If the camera is configured to allow anonymous view, a remote, unauthenticated attacker could exploit this by sending a maliciously crafted request to the server. A successful attack may result in arbitrary command execution or arbitrary file read.
ThinkPHP 5.x Remote Code Execution	T1190	2019-9082	This audit exploits a remote command execution vulnerability in ThinkPHP 5.x less than v5.0.23, v5.1.31. The vulnerability is due to improper validation of parameters in a HTTP GET request. A remote, unauthenticated attacker could exploit this by sending a maliciously crafted request to the server. A successful attack may result in arbitrary command execution in the context of the server process.
Apache Kylin '/migrate' API OS Command Injection	T1190	2020-1956	A command injection vulnerability exists in in Apache Kylin project versions 2.3.0-2.3.2, 2.4.0-2.4.1, 2.5.0-2.5.2, 2.6.0-2.6.4 and 3.0.0. The vulnerability is due to lack of validation for user-supplied input to 'migrate' REST API endpoint. A remote authenticated attacker may execute arbitrary commands by sending a crafted POST request.

Assessment Name: Web Application Script Injection

Audit Name	MITRE ATT&CK	CVE	Info
ThinkPHP 5.x Remote Code Execution	T1190	2019-9082	This audit exploits a remote command execution vulnerability in ThinkPHP 5.x less than v5.0.23, v5.1.31. The vulnerability is due to improper validation of parameters in a HTTP GET request. A remote, unauthenticated attacker could exploit this by sending a maliciously crafted request to the server. A successful attack may result in arbitrary command execution in the context of the server process.

Assessment Name: Web Browser - Google Chrome

Audit Name	MITRE ATT&CK	CVE	Info
Google Chrome WebAudio OfflineAudioContext Use After Free	T1189	2019-13720	This audit exploits a use-after-free vulnerability in the WebAudio component of Google Chrome. The vulnerability is due to incorrect handling of AudioContext objects in memory. A malicious attacker can exploit this vulnerability by creating a specially-crafted HTML page and convince the target user to access it using Chrome. Successful exploitation can potentially lead to remote code execution.

Assessment Name: Web Server Vulnerability

Audit Name	MITRE ATT&CK	CVE	Info
Apache Kylin '/migrate' API OS Command Injection	T1190	2020-1956	A command injection vulnerability exists in in Apache Kylin project versions 2.3.0-2.3.2, 2.4.0-2.4.1, 2.5.0-2.5.2, 2.6.0-2.6.4 and 3.0.0. The vulnerability is due to lack of validation for user-supplied input to 'migrate' REST API endpoint. A remote authenticated attacker may execute arbitrary commands by sending a crafted POST request.

Assessment Name: Malware File Transfer - HTTP (1)

Audit Name	Info
Malware: Snake variant 1	SNAKE, also known as EKANS, is a ransomware that encrypts all processes related to SCADA Systems, Virtual Machines, Industrial Control Systems, Remote Management Tools, and other various Network Software on a system. The purpose of this ransomware is to go after all devices that are connected to the target and not one speciifc machine. The malware is written in GOLANG and contains a higher level of obfuscation than typically seen in ransomware.

Assessment Name: Reflected XSS Efficiency - Group 1 (180)

Audit Name	Info
Reflected XSS Vectors: Payload #3021 - #3200	This audit simulates the sending of a Cross-Site Scripting (XSS) payload.

Release 1.0.5 (2020-07-20)

New Assessments (2)

Assessment Name	Category	Info
Maze Ransomware April 2020 Campaign	Kill-Chain	Maze ransomware has been disclosed since 2019. The ransomware was initially distributed via spam emails and exploit kits and more than 100 companies became victims. Nearly every industry sector including manufacturing, legal, financial services, construction, healthcare, technology, retail, and government has been impacted. For a more detailed analysis of the malware, visit https://www.fireeye.com/blog/threat-research/2020/05/tactics-techniques-procedures-associated-with-maze-ransomware-incidents.html. The scenario in this assessment contains the following steps: 1. A malicious Word Document with an embedded Macro script is delivered to the user. 2. Once a user has opened the document, the Maze malware is downloaded via an HTTP GET request. 3. The malware, once executed, begins to issue Command and Control commands. It performs 2 Maze CNC POST requests. Both requests are sent with binary data which contains host fingerprint information such as host name and user name.
Reflected XSS Efficiency - XSS Vectors	Instrumentation	Cross-Site Scripting (XSS) is a type of computer security vulnerability found in websites that enables attackers to inject scripts into web pages viewed by other users. When these scripts are viewed and executed by other users, they can steal credentials, sensitive data, or modify values or settings on the target website. Reflected XSS (known also as non-persistent XSS) is taking place when the script is not stored on the Web Application side. Typically, the XSS code is spread by sharing a link which is referring a vulnerable web page. The link itself includes the malicious code to execute in web browsers. This assessment contains a collection of Cross-Site Scripting payloads sourced from https://gist.github.com/kurobeats/9a613c9ab68914312cbb415134795b45

New Audits (28)

Assessment Name: Maze Ransomware April 2020 Campaign

Audit Name	MITRE ATT&CK	Info
Maze Apr 2020 Campaign - Word Malware File Transfer	T1189	This audit simulates the download of a Word document containing embedded macros via an HTTP GET request. The macros can be used to download additional malware, like the Maze ransomware seen in the 'Maze Apr 2020 Campaign'.
Maze Apr 2020 Campaign - Maze Malware File Transfer	T1189	This audit simulates the download of the Maze ransomware via an HTTP GET request.

Audit Name	MITRE ATT&CK	Info
Maze Apr 2020 Campaign - Command and Control	T1048	This audit simulates the 'Maze Apr 2020 Campaign - Command and Control' traffic that occurs after executing the 'Maze' ransomware executable. The victim sends an HTTP POST request with binary data containing host information, and the attacker replies with an HTTP code 404. This sequence occurs 2 times.

Assessment Name: Reflected XSS Efficiency - XSS Vectors

Audit Name	MITRE ATT&CK	Info
Reflected XSS: Cheat Sheet Payload #3001 - #3020	T1189	These 20 audits simulate the sending of various Cross-Site Scripting (XSS) payloads.

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

Audit Name	MITRE ATT&CK	CVE	Info
Microsoft Windows SMB DataDisplacement Buffer Overflow	T1190	2017-0143	This audit exploits a vulnerability in parsing an SMBv1 Write AndX Request. A remote, unauthenticated attacker could exploit this vulnerability to execute arbitrary code on the target system. This vulnerability was exploited by the ransomware codenamed "WannaCry" to infect Microsoft Windows - based hosts. The exploit (named Eternal Blue) was leaked by the Shadow Brokers hacking group in April 14, 2017.

Assessment Name: Malicious Office Documents

Audit Name	MITRE ATT&CK	CVE	Info
Microsoft .NET Framework XPS FileParsing Remote Code Execution	T1189	2020-0605	A code execution vulnerability exists in some versions of Microsoft .NET Framework. The vulnerability is due to insecure deserialization of XPS files by the 'XamlReader::Load()' function within 'PresentationFramework.dll'. A remote attacker could exploit this vulnerability by enticing a target user to download and open a crafted XPS file, which may result in the execution of arbitrary code.

Assessment Name: Web Browser - Microsoft

Audit Name	MITRE ATT&CK	CVE	Info
Microsoft Internet Explorer 'comparator' sort method Use-After-Free	T1189	2020-0674	This audit exploits a vulnerability in the Microsoft Internet Explorer scripting engine. Specifically, an attacker can craft an HTML page containing a Javascript script which creates an array of objects, and the object is reassigned in a custom sort function which then calls 'CollectGarbage()' resulting in use after free condition due to a dangling pointer. A remote attacker could exploit this vulnerability by enticing the target user to open a specially crafted web page. Successful

Audit Name	MITRE ATT&CK	CVE	Info
			exploitation could lead to arbitrary code execution in the security context of the target user.

Assessment Name: Web Browser - Apple Safari

Audit Name	MITRE ATT&CK	CVE	Info
Apple Safari WebKit Incorrect ArithNegate Leads to Out Of Bounds Access	T1189	2020-9802	This audit exploits a vulnerability in Apple Webkit. Specifically, an attacker can craft JavaScript in such a way that Checked and Unchecked ArithNegate operations are incorrectly swapped during Common Subexpression Elimination. This will lead to out-of-bounds memory access on an array after being JIT compiled.

Assessment Name: Web Browser - Google Chrome

Audit Name	MITRE ATT&CK	CVE	Info
Google Chrome ReadableStream::Close Out of Bounds Memory Access	T1189	2020-6390	This audit exploits a vulnerability in Google Chrome. Specifically, an attacker can craft JavaScript in such a way that when read_requests are modified from inside the accessor, the loop's iterator becomes invalid, and continuing to iterate through will cause out of bounds memory to be accessed. This can cause a denial of service condition in the browser or potentially lead to remote code execution.

Release 1.0.4 (2020-06-29)

New Assessments (2)

Assessment Name	Category	Info
Authentication Bypass	Instrumentation	Authentication Bypass refers to an attacker gaining access to application, service, or device with the privileges of an authorized or privileged user by evading or circumventing an authentication mechanism. This assessment contains a collection of Authentication Bypass attacks. The effects of a successful attack include access to protected data, disclosure of legally protected, highly sensitive information, even system compromise. It will run through each of the audits one-by-one in order to test how well your implemented security controls protect your assets against these attacks. If these audits are not blocked, they could compromise your web application and/or put your customers and data at risk. * 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.
Data Exfiltration - PII via Zoom Meeting	Instrumentation	This assessment will attempt to exfiltrate an Excel spreadsheet containing PII (Personally Identifiable Information) for over a thousand individuals via Zoom Meeting file upload feature. Each of the audits in this assessment modifies or compresses the original file using a method or technique frequently associated with APT software or well-known threat actors. * If an audit results in Pass, this indicates one of the tested security controls prevented the exfiltration. * If an audit results in Failure, this indicates that all tested security controls failed to prevent the exfiltration.

New Audits (10)

Assessment Name: Authentication Bypass

Audit Name	MITRE ATT&CK	CVE	Info
Wordpress Plugin BBPress Unauthenticated Privilege Escalation	T1190	2020-13693	An authentication bypass vulnerability exists in the bbPress Wordpress plugin. The vulnerability is due to lack of validation on user authorization requests. A remote unauthorized attacker can exploit this vulnerability by

Audit Name	MITRE ATT&CK	CVE	Info
			sending a crafted HTTP POST request to the system. Successful exploitation results in creating a user with full privileges ('Keymaster' role).

Assessment Name: Web Application OS Command Injection

Audit Name	MITRE ATT&CK	CVE	Info
TP-Link NC2XX 'sysname' OS Command Injection	T1190	2020-12109	A remote command injection vulnerability exists in multiple TP-Link Cloud Camera devices (NC2XX) due to lack of user input sanitization. By sending a crafted 'sysname' POST parameter to '/setsysname.fcgi' path, a remote authenticated commander may execute arbitrary commands on the target system.
VMware Cloud Director Expression Language Authenticated Java template injection	T1190	2020-3956	A command injection vulnerability exists in VMware Cloud Director. The vulnerability is due to the lack of sanitization while parsing input passed to 'hostname' parameter within the SMTP configuration form. An authenticated attacker can exploit this vulnerability by crafting a malicious HTTP PUT request. Successful exploitation results in full control of the cloud director platform.

Assessment Name: Data Exfiltration - PII via Zoom Meeting

Audit Name	Info
PII Data Exfiltration via Zoom Meeting - Format: .csv	This audit uploads a file containing PII in a Zoom Meeting. The file consists of an Excel spreadsheet containing PII for more than 1000 individuals as a CSV (Comma-Separated Values) file.
PII Data Exfiltration via Zoom Meeting - Format: .xlsx	This audit uploads a file containing PII in a Zoom Meeting. The file consists of an Excel spreadsheet containing PII (names, email addresses, birth dates, and social security numbers) for more than 1000 individuals.
PII Data Exfiltration via Zoom Meeting - Format: .zip	This audit uploads a file containing PII in a Zoom Meeting. The file consists of an Excel spreadsheet containing PII (names, email addresses, birth dates, and social security numbers) for more than 1000 individuals in .zip format.
PII Data Exfiltration via Zoom Meeting - Format: .tar	This audit uploads a file containing PII in a Zoom Meeting. The file consists of an Excel spreadsheet containing PII (names, email addresses, birth dates, and social security numbers) for more than 1000 individuals in .tar format.
PII Data Exfiltration via Zoom Meeting - Format: .7z	This audit uploads a file containing PII in a Zoom Meeting. The file consists of an Excel spreadsheet containing PII (names, email addresses, birth dates, and social security numbers) for more than 1000 individuals in .7z format.
PII Data Exfiltration via Zoom Meeting - Format: .rar	This audit uploads a file containing PII in a Zoom Meeting. The file consists of an Excel spreadsheet containing PII (names, email addresses, birth dates, and social security numbers) for more than 1000 individuals in .rar format.
PII Data Exfiltration via Zoom Meeting - Format: .jar	This audit uploads a file containing PII in a Zoom Meeting. The file consists of an Excel spreadsheet containing PII (names, email addresses,

Audit Name	Info
	birth dates, and social security numbers) for more than 1000 individuals in .jar format.

Release 1.0.3 (2020-06-16)

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

Need help? Connect with us and we will gladly assist you.

You can contact us by email via threatsim-support@keysight.com or using one of the global or regional support emails and/or phone numbers.

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