



Threat Level

 Red

 CISA: AA23-352A

HiveForce Labs

THREAT ADVISORY



ATTACK REPORT

Play Ransomware A Global Threat Impacting Businesses

Date of Publication

December 19, 2023

Admiralty Code

A1

TA Number

TA2023510

Summary

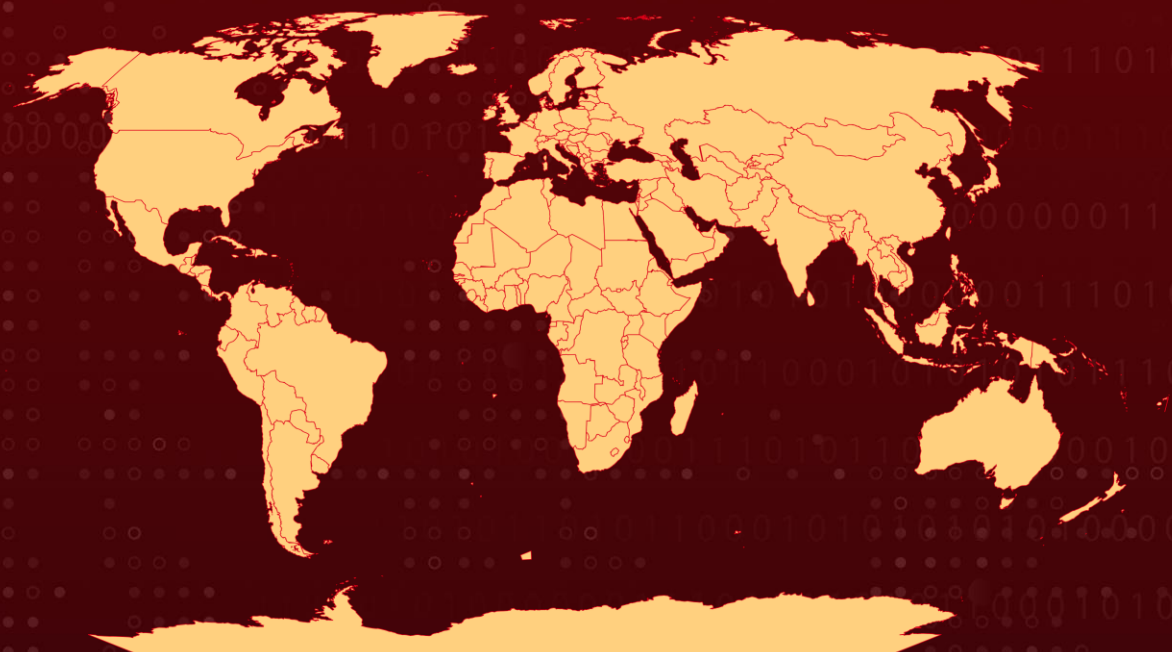
Attack Began: June 2022

Attack Region: North America, South America, Europe, and Australia

Malware: Play Ransomware (also known as Playcrypt)







Attack: The Play ransomware group, active since June 2022, employs a double-extortion model, impacting businesses globally. Utilizing legitimate tools for malicious activities, the group has affected approximately 300 entities.







Attack Regions



Powered by Bing
© Australian Bureau of Statistics, GeoNames, Microsoft, Navinfo, Open Places, OpenStreetMap, TomTom, Zenrin

CVEs

CVE	NAME	AFFECTED PRODUCT	ZERO -DAY	CISA KEV	PATCH
CVE-2018-13379	Fortinet FortiOS SSL VPN Path Traversal Vulnerability	Fortinet FortiOS			
CVE-2020-12812	Fortinet FortiOS SSL VPN Improper Authentication Vulnerability	Fortinet FortiOS			

CVE	NAME	AFFECTED PRODUCT	ZERO -DAY	CISA KEV	PATCH
CVE-2022-41040	Microsoft Exchange Server Server-Side Request Forgery Vulnerability (ProxyNotShell)	Microsoft Exchange Server			
CVE-2022-41082	Microsoft Exchange Server Remote Code Execution Vulnerability (ProxyNotShell)	Microsoft Exchange Server			

Attack Details

#1

The Play ransomware group, also known as Playcrypt, has been active since June 2022, targeting businesses and critical infrastructure in North America, South America, Europe, and, more recently, Australia. As of October 2023, approximately 300 entities have been affected, according to the FBI. The group operates as a closed organization to ensure the secrecy of its activities and employs a double-extortion model, encrypting systems after exfiltrating data.

#2

The Play ransomware group gains initial access to victim networks through the abuse of valid accounts and exploiting vulnerabilities in public-facing applications, such as FortiOS and Microsoft Exchange. The actors use various tools for discovery, defense evasion, lateral movement, and execution, including AdFind, Grixba, Cobalt Strike, Mimikatz, and others.

#3

The ransomware actors exfiltrate data by compressing files with WinRAR and transferring them using WinSCP. The encryption process involves AES-RSA hybrid encryption, with intermittent encryption of every other file portion. The encrypted files receive a .play extension, and a ransom note is placed in the file directory.

#4

Victims are directed to contact the Play ransomware group via email for ransom payment in cryptocurrency. If payment is not made, the threat actors threaten to publish the exfiltrated data on their Tor network leak site. The group utilizes legitimate tools like AdFind, Bloodhound, PsExec, and others, repurposing them for malicious activities.

Recommendations



Implement Robust Endpoint Protection: Deploy advanced endpoint protection solutions that include behavior-based detection, machine learning algorithms, and threat intelligence. These solutions can detect and block malicious activities associated with Play ransomware, such as file encryption and unauthorized processes. Regularly update endpoint security software to ensure protection against the latest threats.



Patch and Update Software: Keep all operating systems, applications, and firmware up to date with the latest security patches and updates. Play affiliates often exploit known vulnerabilities to gain initial access to systems. By promptly applying patches, organizations can mitigate the risk of these vulnerabilities being exploited and prevent unauthorized access to their networks.



Conduct Regular Data Backups and Test Restoration: Implement a robust data backup strategy that includes regular backups of critical data and systems. Ensure backups are stored offline or in a secure, isolated environment to prevent them from being compromised in the event of an attack. Regularly test the restoration process to verify the integrity and availability of backups.



Multi-Factor Authentication (MFA): Require the use of multi-factor authentication (MFA) for all services, especially for email, virtual private networks, and accounts with access to critical systems. MFA enhances security by requiring multiple verification methods.

Potential MITRE ATT&CK TTPs

<u>TA0001</u> Initial Access	<u>TA0010</u> Exfiltration	<u>TA0005</u> Defense Evasion	<u>TA0007</u> Discovery
<u>TA0006</u> Credential Access	<u>TA0008</u> Lateral Movement	<u>TA0009</u> Collection	<u>TA0040</u> Impact
<u>TA0011</u> Command and Control	<u>T1190</u> Exploit Public-Facing Application	<u>T1078</u> Valid Accounts	<u>T1133</u> External Remote Services
<u>T1016</u> System Network Configuration Discovery	<u>T1518.001</u> Security Software Discovery	<u>T1518</u> Software Discovery	<u>T1562.001</u> Disable or Modify Tools

<u>T1562</u> Impair Defenses	<u>T1070.001</u> Clear Windows Event Logs	<u>T1070</u> Indicator Removal	<u>T1552</u> Unsecured Credentials
<u>T1003</u> OS Credential Dumping	<u>T1570</u> Lateral Tool Transfer	<u>T1484.001</u> Group Policy Modification	<u>T1484</u> Domain Policy Modification
<u>T1560.001</u> Archive via Utility	<u>T1560</u> Archive Collected Data	<u>T1484</u> Domain Policy Modification	<u>T1048</u> Exfiltration Over Alternative Protocol

✂ Indicators of Compromise (IOCs)

TYPE	VALUE
MD5	09f341874f72a5cfcedbca707bfd1b3b, 57bcb8cfad510109f7ddedf045e86a70
SHA1	6e8582faeaf34f63fbe0083a811bcce1aa6c31de, e6c381859f53d0c0db9fcd30fa601ecb935b93e0
IPv4	85.203.44[.]5, 85.203.44[.]8
SHA256	453257c3494addafb39cb6815862403e827947a1e7737eb8168cd105224 65deb, 47c7cee3d76106279c4c28ad1de3c833c1ba0a2ec56b0150586c7e8480cc ae57, 75404543de25513b376f097ceb383e8efb9c9b95da8945fd4aa37c7b2f22 6212, 7a42f96599df8090cf89d6e3ce4316d24c6c00e499c8557a2e09d61c00c1 1986, 7a6df63d883bbccb315986c2cfb76570335abf84fafbefce047d126b32234 af8, 7dea671be77a2ca5772b86cf8831b02bff0567bce6a3ae023825aa40354f 8aca, c59f3c8d61d940b56436c14bc148c1fe98862921b8f7bad97fbc96b31d71 193c, e652051fe47d784f6f85dc00adca1c15a8c7a40f1e5772e6a95281d8bf3d5 c74, e8d5ad0bf292c42a9185bb1251c7e763d16614c180071b01da742972999 b95da

Patch Links

<https://fortiguard.com/advisory/FG-IR-18-384>

<http://www.fortiguard.com/psirt/FG-IR-20-233>

<https://fortiguard.com/psirt/FG-IR-19-283>

<https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41040>

<https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41082>

Recent Breaches

www.dywidag-systems.com

www.waldners.com

www.cmpaula.com

www.schoepe-display.com

www.successchoonmaak.nl

www.richardharrislaw.com

www.globalspec.com

www.kuriyama.com

www.ridgewine.com

www.ridegrtc.com

capespan.com

silvent.com

phb.co.uk

www.californiainnovations.com

www.greenwaste.com

gvminc.com

vitroplus.nl

burtonwire.com

planbox.com

agceng.com

www.plslogistics.com

www.ajopartners.com

www.phibro.com

www.intrepidmuseum.org

www.smrinc.com

www.postworks.com

beckerfurnitureworld.com

www.canderel.com

www.labtopiainc.com

www.olace.com

elstonnationwide.com

www.unittransfer.com

schydraulic.com

aiglass.com
thillens.com
www.byfod.com
www.nflandisappliances.com
www.survtechsolutions.com
www.sparex.com
single-point.com
www.moorecoinc.com
www.noblemountain.com
www.edge-re.com
www.cslusa.com
mchalelandscape.com
www.dmc.com
www.kadewe.de
www.wyattdetention.com
www.roadscholar.com
guntert.com
www.piketech.com
www.nomot.nl
trademarkproperty.com
www.thompsonchocolate.com
fgs.com.au
conspare.com
www.albrechtco.com
gtrcomposites.com
www.designa.com
www.ackerman-estvold.com
www.conditionedair.com
www.crownsupply.com
www.idproducts.com
www.mrwilliams.com
www.meindl.de
www.inclinators.com
www.thesupplyroom.com
www.hovhomes.com
www.geopointsurvey.com
www.gspcomponents.com
www.jdrm.com
www.hilyards.com
www.ricardo.com
www.graininspection.com
www.craft-maid.com
www.bry-air.com

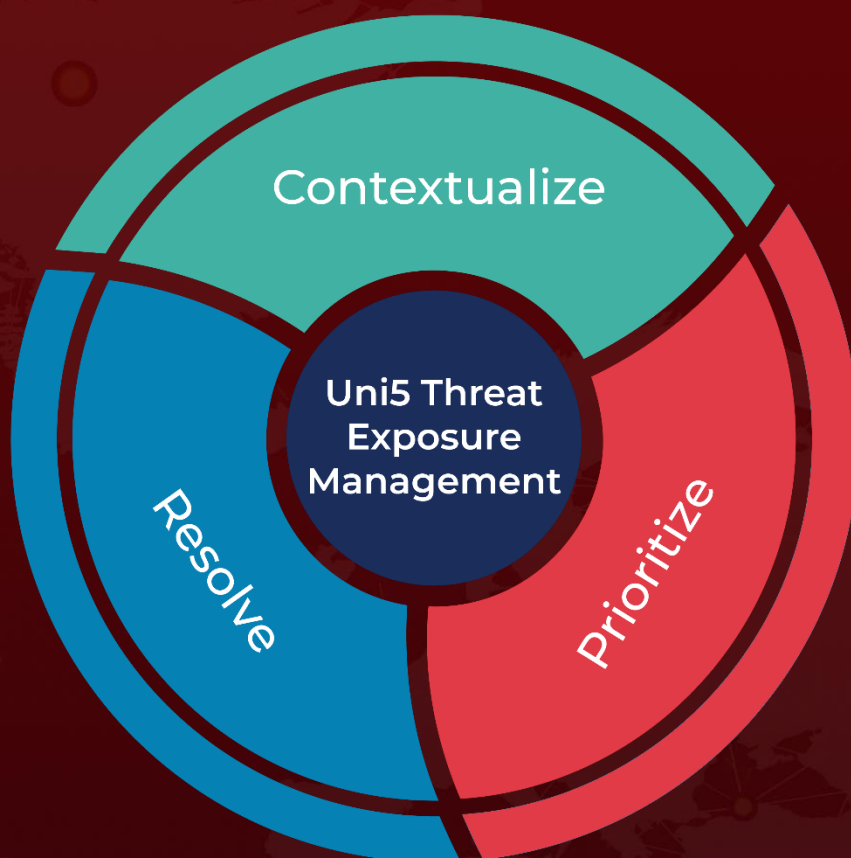
References

<https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-352a>

What Next?

At Hive Pro, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with HivePro Uni5: Threat Exposure Management Platform.



REPORT GENERATED ON

December 19, 2023 • 4:00 AM

© 2023 All Rights are Reserved by Hive Pro®



More at www.hivepro.com