

PlayCrypt Ransomware-as-a-Service Expands Threat from Script Kiddies and Sophisticated Attackers - N-able

By N-able

Published: 2023-11-21 · Archived: 2026-04-02 12:34:42 UTC

Play, also known as “PlayCrypt,” was [discovered last summer](#) disrupting government agencies in Latin America. Months later threat actors began using it for targets in the U.S. and Europe. Play, like most ransomware today, employs double-extortion tactics, stealing victim data before encrypting their networks.

Since August, the Adlumin MDR team has tracked separate Play ransomware attacks in different industries. **In the attacks we observed, threat actors used the same tactics, techniques, and procedures (TTP) and followed the same order of steps — almost identically. Furthermore, the indicators of compromise (IOCs) for both incidents were almost indistinguishable.**

One of those IOCs includes threat actors using the public music folder (C:\...\public\music) to hide malicious files. Another was using almost the same password to create high privilege accounts. And, in both attacks, many of the same commands were observed.

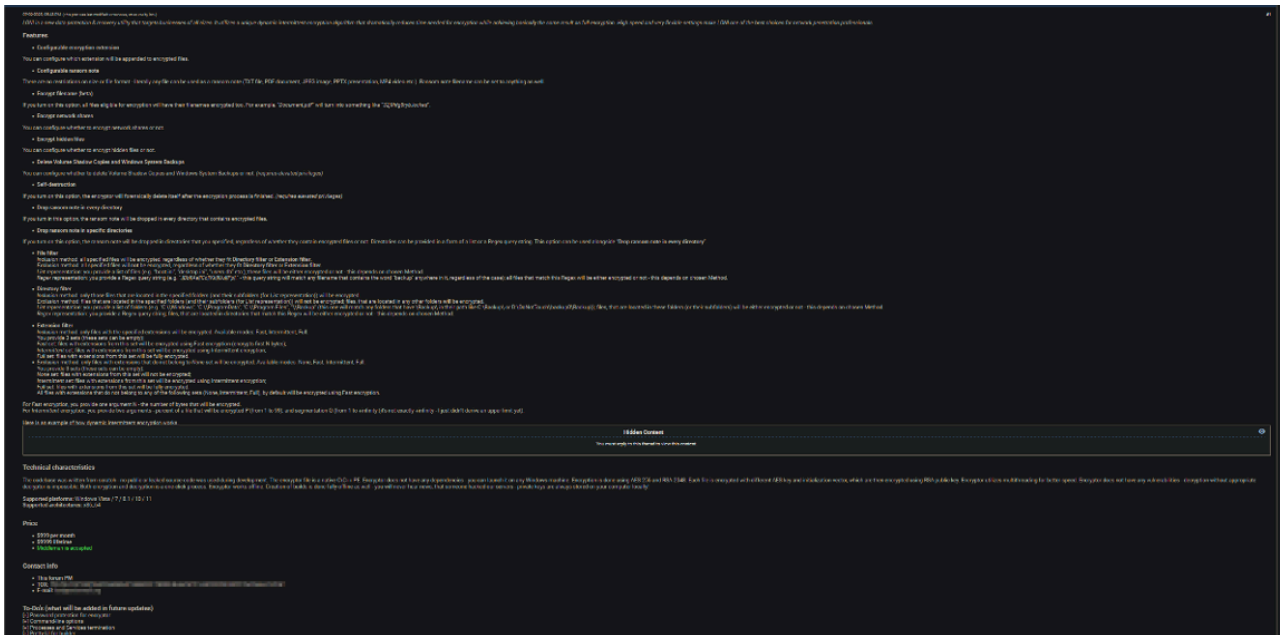
This high level of consistency in methods used by threat actors is telling. First, it highly suggests reliance on playbooks or step-by-step instructions supplied with RaaS kits. And second, the targeted victims shared a common profile; they were smaller organizations that possessed the financial capacity to entertain ransoms reaching or exceeding \$1 million.

The RaaS Kit Market

Purchasing RaaS kits is not difficult, it simply requires a TOR connection and membership to the right dark net forum or market. Once there, a highly experienced threat actor, or even a “script kiddie,” can browse RaaS advertisements.

Below are two ads that we acquired from RaaS operators peddling their products in the dark web.





Other ransomware ads obtained included those that offered “set-up assistance” “for as low as \$200,” and those with “no fees.” Our team also observed advertisements offering full builds from \$300 to \$1100 “ready for deployment.”

One of the ads described the malware being offered as using “many cutting-edge evasion techniques including proprietary methods.”

And in some ads, RaaS operators boasted having ransomware kits for targeting MacOS systems.

“We have developed a new MacOS ransomware as we noticed a lack of it,” the ad read.

At least one post, stated that the ransomware for sale was what “the cool kids are using,” alluding that someone doesn’t have to be “cool” – or perhaps, highly skilled – to purchase and use it.

Easy Enough for a Script Kiddie

Script kiddies are individuals who possess fundamental hacking skills and the knowledge to deploy and execute exploits written by experienced threat actors. They’re able to learn new skills easily and eventually, often become “real hackers” themselves.

Since 2015, researchers have written about the ability script kiddies have for deploying ransomware and often working side-by-side with well-known threat actor organizations.

In March 2022, [police in the UK arrested members of the Lapsus\\$ cybercriminal group](#) known for targeting tech companies such as Okta, Nvidia, Samsung, and Microsoft. The raid included the arrest of teenagers and young adults with ages ranging from 13 to 21, according to the BBC. It’s not clear, however, if the youngsters were script kiddies simply due to their age.

With enough documentation and technical support – and with generative AI tools now being able to assist them as well – a script kiddie can be more than capable of carrying out an attack. However, attacks by these less-skilled

individuals often include a higher degree of basic mistakes that make them easier for an organization with capable cybersecurity operation to stop.

For example, we have observed ransomware attacks foiled by the Adlumin Security Operations Platform or the Adlumin MDR Team during an attack's early stages. **In some cases, threat actors don't even get the chance to encrypt files. There are also incidents where SOAR actions within the Adlumin platform disable accounts created by threat actors, effectively locking them out from the network. Sometimes attacks are carried out, but no data is exfiltrated.**

Money to be Made

Ransomware attacks are very lucrative, especially since [73% of companies attacked pay the ransom](#). And with double extortion becoming the norm, organizations that don't pay are publicly shamed by RaaS operators on the clear or dark web.

For script kiddies of any age, ransomware may seem like a great way to make a living and become rich quickly. Also, with high unemployment rates in many countries in Latin America and other parts of the world, cybercrime may be seductive for underemployed or poorly paid computer programmers, or people in similar careers. [According to DevelopmentAid.org](#), “[Poor countries] serve as training grounds for criminal groups in preparation for more ambitious attacks in developed countries.”

When RaaS operators advertise ransomware kits that come with everything a hacker will need, including documentation, forums, technical support, and ransom negotiation support, script kiddies will be tempted to try their luck and put their skills to use. And since there are probably more script kiddies than “real hackers” today, businesses and authorities should take note and prepare for a growing wave of incidents.

Breadcrumbs

IOCs, such as malicious IP addresses, domains, TOR addresses, emails, hashes, executables, and others discovered from an attack can be very useful to analysts, researchers, and law enforcement. They serve as clues to help put together what transpired during the incident and how. They can also offer some insight about the level of sophistication of the attackers.

When threat actors follow RaaS-provided playbooks, they will likely adhere to them closely on the first few attacks. They'll make mistakes, and if those mistakes are big enough, they could serve as breadcrumbs for the authorities to follow.

Anything an attacker does in a network can help authorities if they are contacted after an incident. This is why investigators request that victims share any IOCs that could help with their investigations. Even if a business pays the ransom, details like Bitcoin or Monero addresses and transaction IDs, communication or chat logs with threat actors, the decryptor file, and a sample of an encrypted file can be very useful.

If a newbie or script kiddie isn't meticulous with their work, the FBI could soon be knocking on their door.

Conclusion

Ransomware attacks continue to be among the most prevalent cyber threats and [increased by 37% in 2023](#). Companies should expect more ransomware attacks in the future, not less. And **if more novice attackers are finding that ransomware attacks can be carried out easily with the help and support provided by RaaS operators, they'll continue to frequent dark net forums to join the most inviting ransomware affiliate group.**

At the same time, novice attackers are more likely to make mistakes since they are not as experienced, potentially leaving behind significant IOCs that the authorities can use to help track and apprehend them.

The Adlumin MDR Team will continue to monitor and stop ransomware attacks carried out by newbies and experts alike. Our security operations platform's SOAR actions have been successful at foiling these attacks in their early stages, stopping cybercriminals on their tracks.

Furthermore, we offer Total Ransomware Defense (TRD), a service specifically designed to detect ransomware activity and stop it. In the unfortunate case that files are encrypted, TRD is able to generate decryption keys to restore systems and networks.

Indicators of Compromise (IOCs)

Username

- admon
- daksj
- admin

Objects

- exe
- zip.json.PLAY
- exe
- exe
- PLAY
- exe
- ini.PLAY
- aut
- omaticDestinations-
- PLAY
- exe
- json.PLAY
- cdp.PLAY
- HeartBea
- updatestore51b519d5-b6f5-4333-8df6-e74d7c9aead4.xml.PLAY
- exe
- cookie.PLAY
- js.PLAY

- exe

Paths

C:\\Users\\Public\\Music

\\Device\\HarddiskVolume3\\CollectGuestLogsTemp

Hash: null

C:\\Users\\Public\\Music

Hash:

b042bc03144919c0fed9d60c1f68eb04ed7

2c2f6

C:\\windows

Hash:

51d3d661774cc50bb22e62beafc4bc6029d

f2392

\\Device\\HarddiskVolume2\\Users\\it.ad

min\\AppData\\Local\\Google\\Chrome\\

User Data\\Default\\Cache\\Cache_Data

Hash: null

C:\\Windows

Hash:

51d3d661774cc50bb22e62beafc4bc6029d

f2392

\\Device\\Mup\\10.20.0.15\\C\$\\\$Recycl

e.Bin\\S-1-5-21-3568089881-786281157-

4253494709-1103

Hash: null

\\Device\\HarddiskVolume2\\Users\\AAD

_00864e0326c2\\AppData\\Roaming\\Mi

crosoft\\Windows\\Recent\\AutomaticDe

stinations

Hash: null

C:\\Users\\Public\\Music

Hash:

b042bc03144919c0fed9d60c1f68eb04ed7

2c2f6

\\Device\\Mup\\10.20.0.15\\C\$\\Users\\

administrator\\AppData\\Local\\ConnectedDevicesPlatform

Hash: null

\\Device\\Mup\\10.20.0.15\\C\$\\Package

s\\Plugins\\Microsoft.EnterpriseCloud.Mo

nitoring.MicrosoftMonitoringAgent\\1.0.1

8067.0\\Status

Hash: null

\\Device\\HarddiskVolume2\\ProgramDat

a\\USOPrivate\\UpdateStore

Hash: null

C:\\Users\\Public\\Music

Hash:

b042bc03144919c0fed9d60c1f68eb04ed7

2c2f6

\\Device\\HarddiskVolume2\\Users\\it.ad

min\\AppData\\Local\\Microsoft\\Windo

ws\\INetCookies

Hash: null

\\Device\\HarddiskVolume4\\Program

Files\\Microsoft Monitoring

Agent\\Agent\\APMDOTNETCollector\\W

eb\\Scripts\\V7.0\\js

Hash: null

C:\\PerfLogs

Hash:

b042bc03144919c0fed9d60c1f68eb04ed7

2c2f6

© 2026 N-able Solutions ULC and N-able Technologies Ltd. All rights reserved.

This document is provided for informational purposes only and should not be relied upon as legal advice. N-able makes no warranty, express or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness of any information contained herein.

The N-ABLE, N-CENTRAL, and other N-able trademarks and logos are the exclusive property of N-able Solutions ULC and N-able Technologies Ltd. and may be common law marks, are registered, or are pending registration with the U.S. Patent and Trademark Office and with other countries. All other trademarks mentioned herein are used for identification purposes only and are trademarks (and may be registered trademarks) of their respective companies.

Source: <https://adlumin.com/post/playcrypt-ransomware-as-a-service-expands-threat-from-script-kiddies-and-sophisticated-attackers/>