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

adlumin.com/post/playcrypt-ransomware-as-a-service-expands-threat-from-script-kiddies-and-sophisticated-attackers/

November 21, 2023

Key Takeaways

- Adlumin uncovered evidence that Play ransomware (also known as PlayCrypt) is now being sold "as a service." Play ransomware has been responsible for attacks on companies and government organizations worldwide since it was first discovered in 2022. Making it available to affiliates that might include sophisticated hackers, less-sophisticated "script kiddies" and various levels of expertise in between, could dramatically increase the volume of attacks using the highly successful, Russia-linked Play ransomware.
- In recent months, Adlumin has identified and stopped PlayCrypt attacks that had nearly identical tactics, techniques and procedures (TTPs). The unusual lack of even small variations between attacks suggests that they are being carried out by affiliates who have purchased the ransomware-as-a-service (RaaS) and are following step-by-step instructions from playbooks delivered with it.
- Based on the attacks Adlumin has witnessed, small and mid-sized organizations are being targeted and are especially at risk. However, ransomware delivered as a service can often be easier to detect because of the common methods used to deploy it. Security teams should watch for indicators of compromise (IOCs) including malicious IP addresses, domains, TOR addresses, emails, hashes and executables, including the ones identified in the article below.

The Patterns

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 Adlumin 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.**

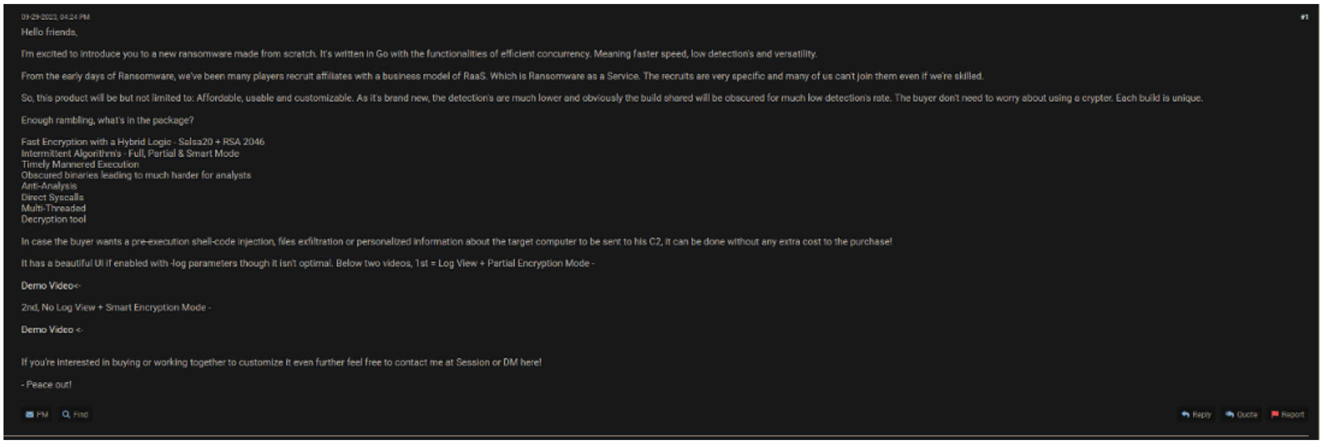
One of those IOCs includes threat actors using the public music folder (C:\…\public\music) to hide malicious files. Another was using almost the same password to create high privilege accounts. And, in both attacks, many of the same commands were observed.

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 Adlumin acquired from RaaS operators peddling their products in the dark web.



09-29-2023, 04:24 PM

#1

Hello friends,

I'm excited to introduce you to a new ransomware made from scratch. It's written in Go with the functionalities of efficient concurrency. Meaning faster speed, low detection's and versatility.

From the early days of Ransomware, we've been many players recruit affiliates with a business model of RaaS. Which is Ransomware as a Service. The recruits are very specific and many of us can't join them even if we're skilled.

So, this product will be but not limited to: Affordable, usable and customizable. As it's brand new, the detection's are much lower and obviously the build shared will be obscured for much low detection's rate. The buyer don't need to worry about using a crypter. Each build is unique.

Enough rambling, what's in the package?

Fast Encryption with a Hybrid Logic - Salsa20 + RSA 2046
Intermittent Algorithm's - Full, Partial & Smart Mode
Timely Mannered Execution
Obscured binaries leading to much harder for analysts
Anti-Analysis
Direct Syscalls
Multi-Threaded
Decryption tool

In case the buyer wants a pre-execution shell-code injection, files exfiltration or personalized information about the target computer to be sent to his C2, it can be done without any extra cost to the purchase!

It has a beautiful UI if enabled with -log parameters though it isn't optimal. Below two videos, 1st = Log View + Partial Encryption Mode -

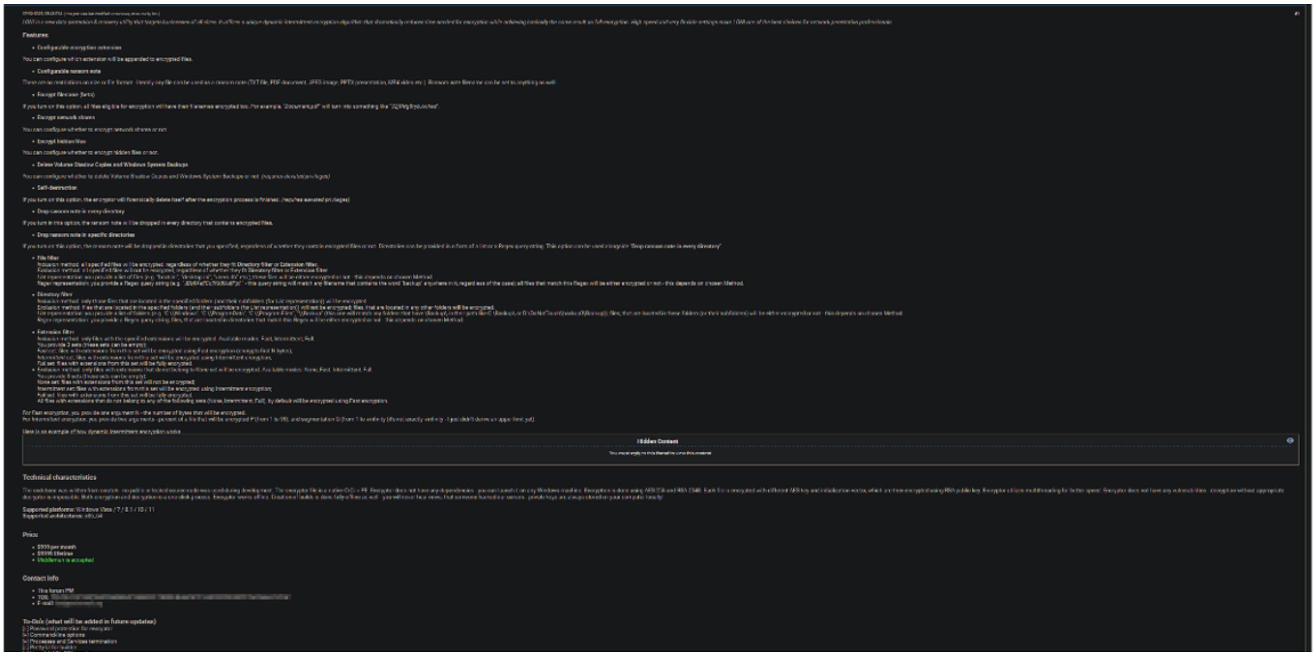
Demo Video<-

2nd, No Log View + Smart Encryption Mode -

Demo Video <-

If you're interested in buying or working together to customize it even further feel free to contact me at Session or DM here!

- Peace out!



[illegible] is a new data protection & recovery utility that targets businesses of all sizes. It offers a unique dynamic intermittent encryption algorithm that dramatically reduces time needed for encryption while achieving [illegible] the same result as full encryption. High speed and very flexible settings make [illegible] one of the best choices for network penetration professionals.

Features:

- **Configurable encryption extension**

You can configure which extension will be appended to encrypted files.

- **Configurable ransom note**

There are no restrictions on a size or file format - literally any file can be used as a ransom note (TXT file, PDF document, JPEG image, PPTX presentation, MP4 video etc.). Ransom note filename can be set to anything as well.

- **Encrypt filenames (beta)**

If you turn on this option, all files eligible for encryption will have their filenames encrypted too. For example, "Document.pdf" will turn into something like "[illegible]".

- **Encrypt network shares**

You can configure whether to encrypt network shares or not.

- **Encrypt hidden files**

You can configure whether to encrypt hidden files or not.

- **Delete Volume Shadow Copies and Windows System Backups**

You can configure whether to delete Volume Shadow Copies and Windows System Backups or not. *(requires elevated privileges)*

- **Self-destruction**

If you turn on this option, the encryptor will forensically delete itself after the encryption process is finished. *(requires elevated privileges)*

- **Drop ransom note in every directory**

If you turn in this option, the ransom note will be dropped in every directory that contains encrypted files.

- **Drop ransom note in specific directories**

If you turn on this option, the ransom note will be dropped in directories that you specified, regardless of whether they contain encrypted files or not. Directories can be provided in a form of a list or a Regex query string. This option can be used alongside "Drop ransom note in every directory"

- File filter
  Inclusion method: all specified files will be encrypted, regardless of whether they fit Directory filter or Extension filter.
  Exclusion method: all specified files will not be encrypted, regardless of whether they fit Directory filter or Extension filter.
  List representation: you provide a list of files (e.g. "boot.ini", "desktop.ini", [illegible] etc.), these files will be either encrypted or not - this depends on chosen Method.
  Regex representation: you provide a Regex query string (e.g. "[illegible]") - this query string will match any filename that contains the word "backup" anywhere in it, regardless of the case; all files that match this Regex will be either encrypted or not - this depends on chosen Method.

- Directory filter
  Inclusion method: only those files that are located in the specified folders (and their subfolders (for List representation)) will be encrypted.
  Exclusion method: files that are located in the specified folders (and their subfolders (for List representation)) will not be encrypted; files, that are located in any other folders will be encrypted.
  List representation: you provide a list of folders (e.g. "C:\\Windows", "C:\\ProgramData", "C:\\Program Files", "\\Backup" (this one will match any folder that have \Backup\ in their path [illegible]); files, that are located in these folders (or their subfolders) will be either encrypted or not - this depends on chosen Method.
  Regex representation: you provide a Regex query string, files, that are located in directories that match this Regex will be either encrypted or not - this depends on chosen Method.

- Extension filter
  Inclusion method: only files with the specified extensions will be encrypted. Available modes: Fast, Intermittent, Full.
  You provide 3 sets (these sets can be empty):
  Fast set: files with extensions from this set will be encrypted using Fast encryption (encrypts first N bytes);
  Intermittent set: files with extensions from this set will be encrypted using Intermittent encryption;
  Full set: files with extensions from this set will be fully encrypted.
- Exclusion method: only files with extensions that do not belong to None set will be encrypted. Available modes: None, Fast, Intermittent, Full.
  You provide 3 sets (these sets can be empty):
  None set: files with extensions from this set will not be encrypted;
  Intermittent set: files with extensions from this set will be encrypted using Intermittent encryption;
  Full set: files with extensions from this set will be fully encrypted.
  All files with extensions that do not belong to any of the following sets (None, Intermittent, Full), by default will be encrypted using Fast encryption.

For Fast encryption, you provide one argument N - the number of bytes that will be encrypted.
For Intermittent encryption, you provide two arguments - percent of a file that will be encrypted P (from 1 to 99), and segmentation S (from 1 to infinity (it's not exactly infinity - I just didn't come up with a limit yet)).

Here is an example of how dynamic intermittent encryption works

Hidden Content

You must reply to this thread to view this content.

Technical characteristics

The codebase was written from scratch - no public or leaked source code was used during development. The encryptor file is a native C/C++ PE. Encryptor does not have any dependencies - you can launch it on any Windows machine. Encryption is done using AES 256 and RSA 2048. Each file is encrypted with different AES key and initialization vector, which are then encrypted using RSA public key. Encryptor utilizes multithreading for better speed. Encryptor does not have any vulnerabilities - decryption without appropriate decryptor is impossible. Both encryption and decryption is a one click process. Encryptor works offline. Creation of builds is done fully offline as well - you will never hear news, that someone hacked our servers - private keys are always stored on your computer locally.

Supported platforms: Windows Vista / 7 / 8.1 / 10 / 11
Supported architectures: x86_64

Price:

- $999 per month
- $9999 lifetime
- Middleman is accepted

Contact info

- This forum PM
- TOX: [redacted]
- E-mail: [redacted]

To-Do's (what will be added in future updates):
[-] Password protection for encryptor
[+] Command-line options
[+] Processes and Services termination
[-] Portable builder

Other ransomware ads obtained included those that offered "set-up assistance" "for as low was $200," and those with "no fees." Adlumin 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, Adlumin has observed ransomware attacks foiled by its security operations platform or its 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, Adlumin now offers 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)

Usernames

- 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